BIPAC 6600

Broadband Firewall Router

User Manual

Table of Contents

Chapter 1 1

INTRODUCTION 1

1.1 An Overview of BIPAC 6600 1
1.2 Package Contents 2
1.3 BIPAC 6600 Features 2
1.4 BIPAC 6600 Application 3

Chapter 2 4

USING BILLION BROADBAND ROUTER 4

2.1 Cautions for Using Billion Broadband Router 4
2.2 The Front LEDs 4
2.3 The Rear Ports 5
2.4 Cabling 6

Chapter 3 7

CONFIGURATION 7

3.1 Before Configuration 7
3.2 Factory Default Settings 13
3.2.1 Password 13
3.2.2 LAN and WAN Port Addresses 14
3.3 Information from ISP 14
3.4 Configuring with Web Browser 15
3.4.1 Status 16
3.4.1.1 Routing Table 16
3.4.1.2 DHCP Table 17
3.4.1.3 System Log 18
3.4.1.4 Security Log 18
3.4.1.5 UPnP Portmap 19
3.4.2 Quick Start 20
3.4.3 Configuration 21
3.4.3.1 LAN 21
3.4.3.1.1 Ethernet 21
3.4.3.1.2 DHCP Server 22
3.4.3.2 WAN 23
3.4.3.2.1 ISP 23
3.4.3.2.2 DNS 25
3.4.3.3 System 26
3.4.3.3.1 Time Zone 26
3.4.3.3.2 Firmware Upgrade 27
3.4.3.3.3 Backup/Restore Settings 28
3.4.3.3.4 Default Setting 28
3.4.3.3.5 Restart 29
3.4.3.3.6 User Management 30
3.4.3.4 Firewall 30
3.4.3.4.1 Packet Filtering 30
3.4.3.4.2 URL Filtering 32
3.4.3.4.3 MAC Address Filtering 33

3.4.3.4.4 Intrusion Detection....34
3.4.3.4.5 Block WAN Request....35
3.4.3.5 Virtual Server....35
3.4.3.5.1 Port Forwarding....36
3.4.3.5.2 Port Mapping....37
3.4.3.5.3 DMZ....38
3.4.3.6 Advanced....38
3.4.3.6.1 Static Route....38
3.4.3.6.2 Dynamic DNS....40
3.4.3.6.3 Device Management....41
3.4.3.6.4 HELP....41

Chapter 4....43

TROUBLESHOOTING....43
Problems Starting Up the Broadband Router....43
Problems with the LAN Interface....43
Why do I get IP conflict information in my computer?....43
Why won't my Internet application work?....44
Can I upgrade the gateway's firmware?....44
Can I set a fixed IP address on my PC?....44
Is there a tool to check my PC's TCP/IP settings in MS Windows?....44
How can I test the whole path (PC⟷Router⟷outside world) to make sure it works fine?....46
How can I check the active IP settings for my WAN port?....47
Where can I find the WAN port's MAC address?....47
How can I explore a local server to be visible to outside users?....47
What is DMZ host?....48
How to configure my MacOS to surf Internet through BIPAC 6600?....48
How can I do if I forget the password for accessing Router?....48
How can I do if there is already a DHCP server in LAN?....48
How many PCs can share this single BIPAC 6600 simultaneously?....49
Which connection method should I select in WAN-ISP setting window?....49

APPENDIX....50

PRODUCT SUPPORT AND CONTACT INFORMATION....50

Chapter 1
Introduction

1.1 An Overview of BIPAC 6600

BIPAC 6600 functions as an IEEE 802.3 Ethernet-based router. It provides four 10/100Mbps Dual Speed Ethernet ports for connection to a home network and one 10/100Mbps Ethernet port for a DSL Modem, Cable Modem, or other broadband access device.

The product is an integrated Internet IP sharing device with a built-in 4-port 10/100Mbps Base-T N-Way Ethernet switch. It is the perfect solution to connect a small group of PCs to a high-speed broadband Internet connection. Multi-users can have high-speed Internet access simultaneously via one single IP address of the Cable/xDSL modem.

This product also serves as an Internet firewall, protecting your network from being accessed by outside users. Not only provide the natural firewall function (Network Address Translation, NAT), it also provides rich firewall features to secure user's network. All incoming data packets are monitored and filtered. Besides, it can also be configured to block internal users from accessing to the Internet.

The product provides three levels of security support. Firstly, it masks LAN users' IP addresses which are invisible to outside users on the Internet, making it much more difficult for a hacker to target a machine on your network. Secondly it can block and redirect certain ports to limit the services that outside users can access. For example, to ensure that games and other Internet applications will run properly, user can open some specific ports for outside users to access internal services in network. Finally it can also detect and block many Hacker Patterns and not allow hacker into your network.

Integrated DHCP services, client and server, allow up to 253 users to get their IP addresses automatically on boot up from the product. Simply set local machines as a DHCP client to accept a dynamically assigned IP address from DHCP server. Each time local machine is powered up; BIPAC 6600 will recognize it and assign an IP address to instantly connect it to the LAN.

For advanced users, Virtual Server function allows the product to provide limited visibility to local machines with specific services for outside users. An ISP provided IP address can be set to the product and then specific services can be rerouted to specific computers on the local network. For instance, a dedicated web server can be connected to the Internet via the product and then incoming requests for HTML that are received by the product can be rerouted to the dedicated local web server, even though the server now has a different IP address. In this example, the product is on the Internet and vulnerable to attacks, but the server is protected.

Virtual Server can also be used to re-task services to multiple servers. For instance, the product can be set to allow separated FTP, Web, and Multiplayer game servers to share the same Internet-visible IP address while still protecting the servers and LAN users from hackers.

1.2 Package Contents

1. Billion BIPAC 6600 Broadband Firewall Router
2. One CD-ROM containing online manual
3. One Quick Start Guide
4. One CAT-5 straight LAN cable
5. One power adapter

1.3 BIPAC 6600 Features

BIPAC 6600 Broadband Firewall Router provides the following features:

- **Multi-Protocol to Establish A Connection:** Supports PPP over Ethernet (RFC 2516) and DHCP client to establish a connection with ISP.

- **Quick Installation Wizard:** Supports a WEB GUI page to install this device quickly. With this wizard, an end user can enter the information easily which they receive from the ISP, then surf the Internet immediately.

- **Universal Plug and Play (UPnP) and UPnP NAT Traversal:** This protocol is used to enable simple and robust connectivity among stand-alone devices and PCs from many different vendors. It makes network simple and affordable for users. UPnP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices. With this feature enabled, users can now connect to Net meeting or MSN Messenger seamlessly.

- **Network Address Translation (NAT):** Allows multi-users to access outside resource such as Internet simultaneously with one IP address/one Internet access account. Besides, many application layer gateway (ALG) are supported such as NetMeeting, PPTP pass-through, IPSec pass-through, etc.

- **Dynamic Domain Name System (DDNS):** The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address. For example, to use the service, you must first apply an account from this free Web server http://www.dyndns.org/. There are more than 5 DDNS servers supported.

- **PPP over Ethernet (PPPoE):** Provides embedded PPPoE client function to establish a connection. Users can get greater access speed without changing the operation concept, sharing the same ISP account and paying for one access account. No PPPoE client software is required for local computer. The Automatic Reconnect and Disconnect Timeout (Idle Timer) functions are provided, too.

- **Virtual Server:** User can specify some services to be visible from outside users. The router can detect incoming service request and forward it to the specific local computer to handle it. For example, user can assign a PC in LAN acting as WEB server inside and expose it to the outside network. Outside user can browse inside web server directly while it is protected by NAT. A DMZ host setting is also provided to a local computer exposed to the outside network, Internet.

- **Firewall:** Supports SOHO firewall with NAT technology. Automatically detects and blocks the Denial of Service (DoS) attack. The URL-blocking and packet filtering are also supported. The hacker's attack will be recorded associated with timestamp in the security logging area.

- **Dynamic Host Control Protocol (DHCP) client and server:** In the WAN site, the DHCP client can get an IP address from the Internet Server Provider (ISP) automatically. In the LAN site, the DHCP server can allocate multiple clients IP addresses and distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.

- **Rich Packet Filtering:** Not only filter the packet based on IP address, but also based on Port numbers and MAC address. It will increase the performance in LAN and WAN, also provide a higher-level security control

- **SNTP:** An easy way to get the network real time information from an SNTP server.

- **Web based GUI:** Supports web based GUI for configuration and management. It is user-friendly and comes with on-line help. It also supports remote management capability for remote users to configure and manage this product.

1.4 BIPAC 6600 Application

Chapter 2
Using Billion Broadband Router

2.1 Cautions for Using Billion Broadband Router

Do not place the router under high humidity and high temperature.

Do not use the same power source for the device with other equipment.

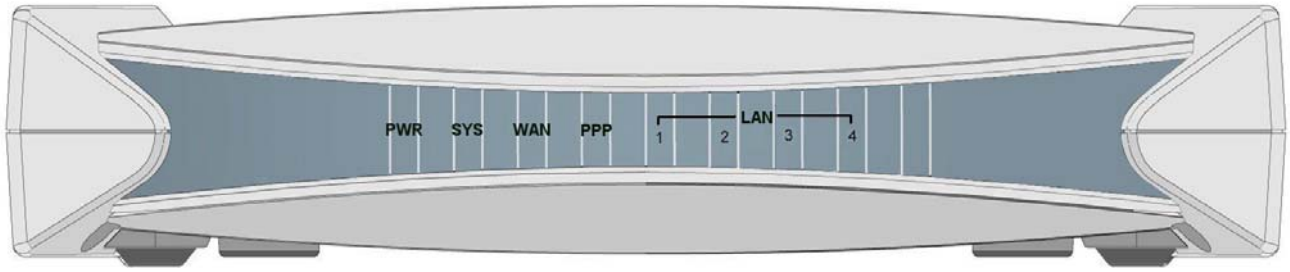
Do not open or repair the case yourself. If the device is too hot, turn off the power immediately and have a qualified serviceman repair it.

Avoid using this product and all accessories outdoors.

Place the product on the stable surface.

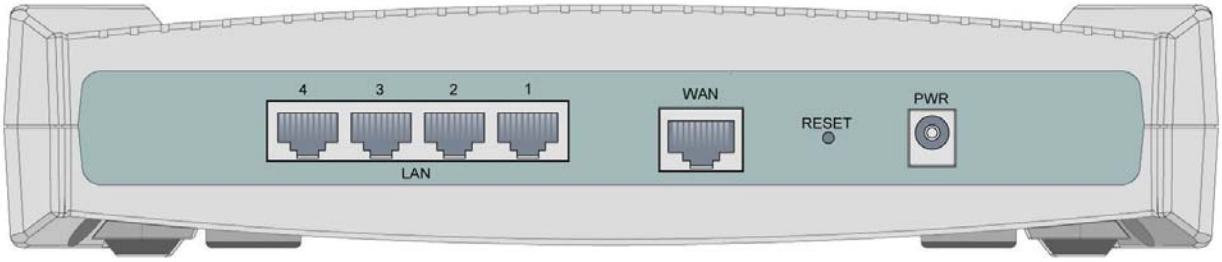
Only use the power adapter that comes with the package.

2.2 The Front LEDs



LED	Meaning
PWR	Lit green when power adapter is connected.
SYS	When lit, it indicates that the device is ready.
WAN	Lit green when connected at 100 Mbps. Lit orange when connected at 10 Mbps. Flashes when sending/receiving data.
PPP	Lit green when PPPoE connection is established
LAN1 **LAN2** **LAN3** **LAN4**	Lit green when the relevant LAN link is connected.

2.3 The Rear Ports



Port	Meaning
PWR	Connect the supplied power adapter to this jack.
RESET	After the device is powered on, press it to reset the device or restore to factory default settings. **0-3 seconds**: reset the device **6 seconds above**: restore to factory default settings (this is used when you can not login to the router, e.g. forgot the password)
WAN	Connect an UTP Ethernet cable to this port when connecting to a hub. Connect a crossover cable to this port when connecting to a DSL/Cable bridge or modem for establishing WAN connections.
LAN **(1x-4x)**	Connect an UTP Ethernet cable to these four ports when connecting to a LAN of 10Mbps or 100Mbps such as an office or home network.

2.4 Cabling

Through Ethernet Port

Please refer to **section 1.4 *"BIPAC 6600 Application"*** first; it gives a clear cable connection diagram.

The most common problem associated with Ethernet is bad cabling. Make sure that all connected devices are turned on. On the top of the product is a bank of LEDs, as a first check, verifies that the relevant LAN Link and WAN Link LEDs are lit. If they are not, verify that you are using the proper cables.

As long as the cables are connected and the LEDs are lit normally, follow section ***"3.2 Configuring the Network Properties"*** below to modify the network settings.

Since the product cannot auto-detect whether your cable is correct or not, please make sure you are using the right cable to a PC or a Hub.

Chapter 3
Configuration

BIPAC 6600 can be configured with your Web browser. The web browser is included as a standard application in following Operation Systems, Windows 95/98/NT/2000/Me/XP, Mac, Unix and Linux. The product provides a very easy and user-friendly interface for configuration.

3.1 Before Configuration

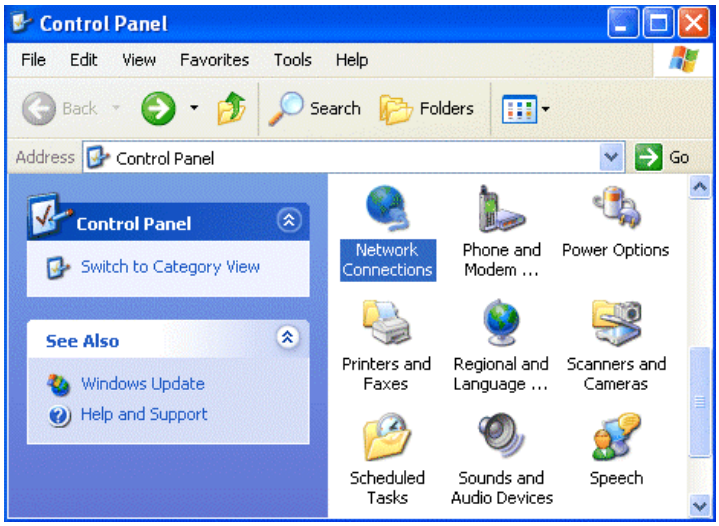
This section describes the configuration required by LAN-attached PCs that communicate with BIPAC 6600, either to configure the device, or for network access. These PCs must have an Ethernet interface installed properly, be connected to BIPAC 6600 either directly or through a hub, and have TCP/IP installed and configured to obtain an IP address through a DHCP server or a fixed IP address which must be in the same subnet of BIPAC 6600. The default IP address of router is **192.168.1.254** and subnet mask is **255.255.255.0**. The best and easy way is to configure the PC to get an IP address from BIPAC 6600.

Please follow the steps below for PC's network environment installation. Before taking the first step, please check your PC's network components. If your PC connects the Broadband Router through Ethernet port, the TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to MS Windows relative manuals.

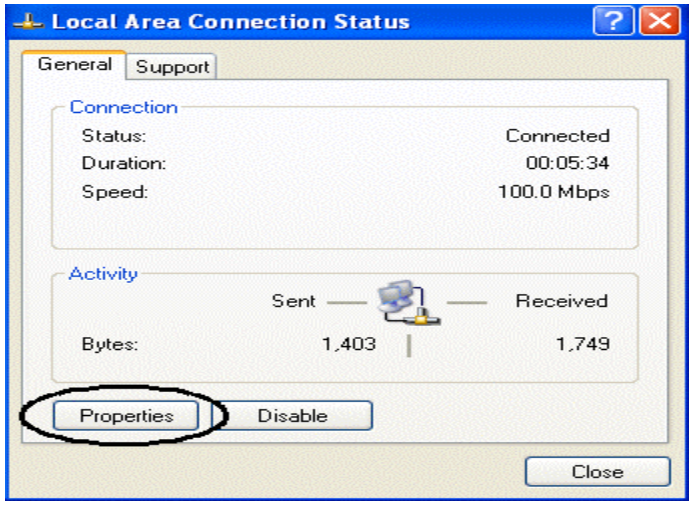
Any TCP/IP capable workstation can be used to communicate with or through BIPAC 6600. To configure other types of workstations, please consult the manufacturer's documentation.

Configuring PC in Windows XP

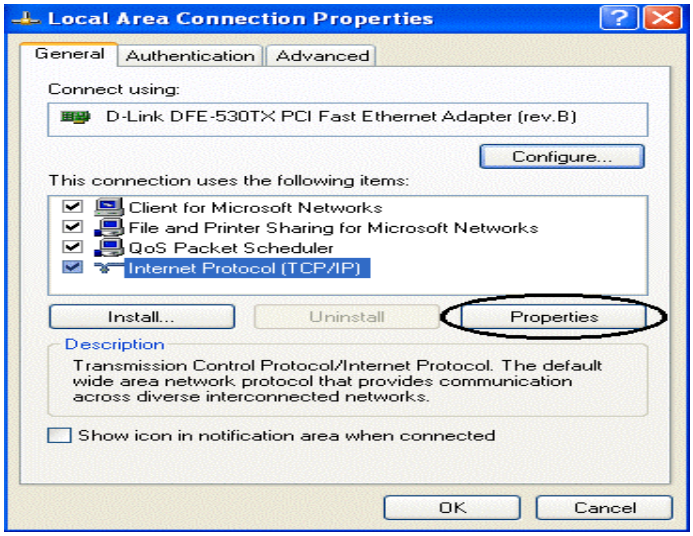
1. Go to **Start / Control Panel (in Classic View)**. In the Control Panel, double-click on **Network Connections.**
2. Double-click **Local Area Connection**.



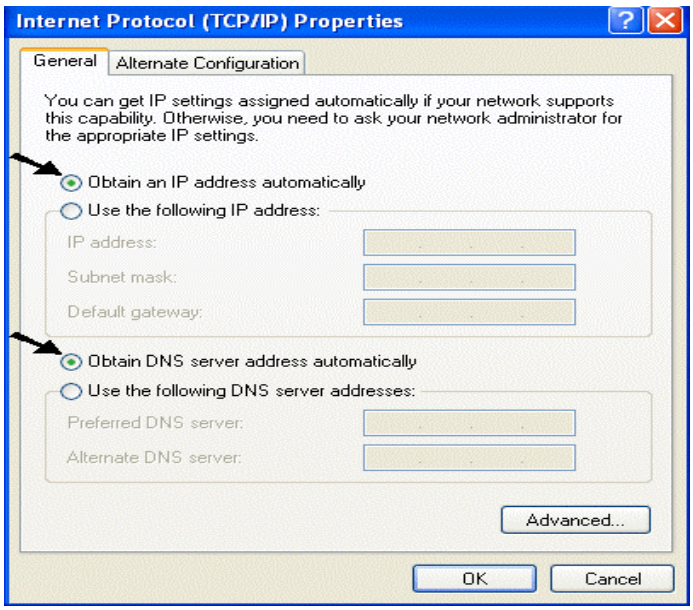
3. In the **Local Area Connection Status** window, click **Properties**.



4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



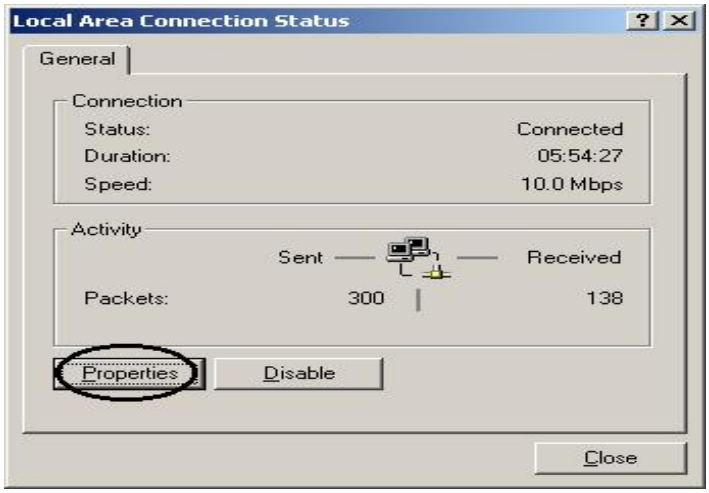
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration.


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

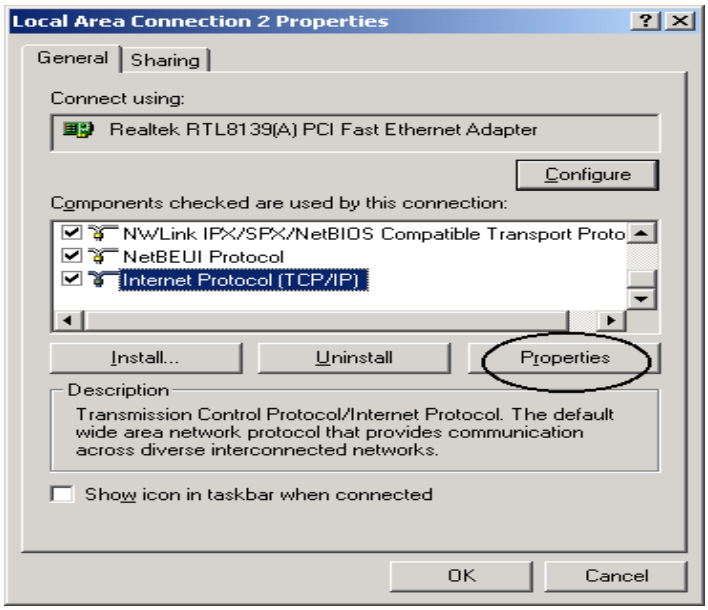
Configuring PC in Windows 2000

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connections**.
2. Double-click **Local Area Connection**.

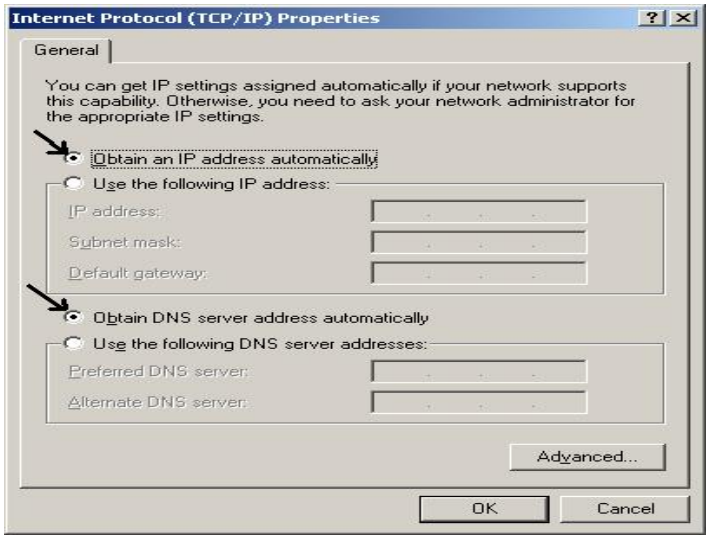
3. In the **Local Area Connection Status** window, click **Properties**.



4. Select **Internet Protocol (TCP/IP)** and click **Properties**.

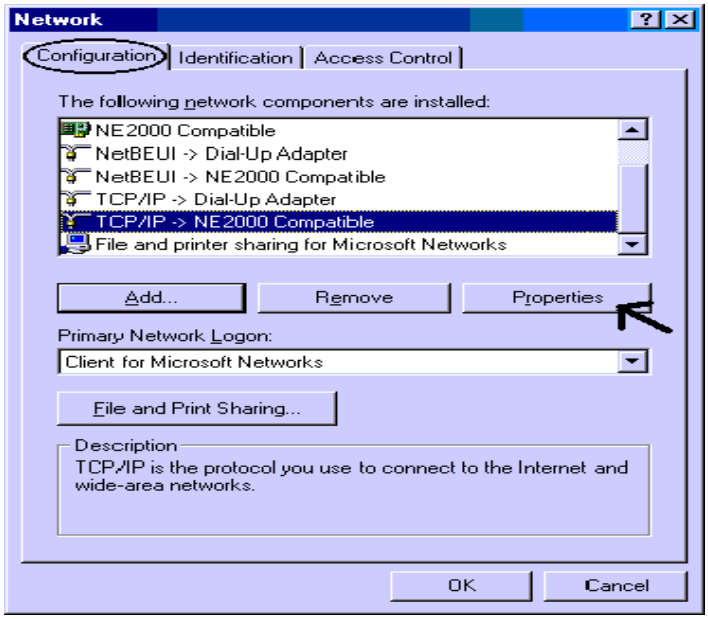


5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration.

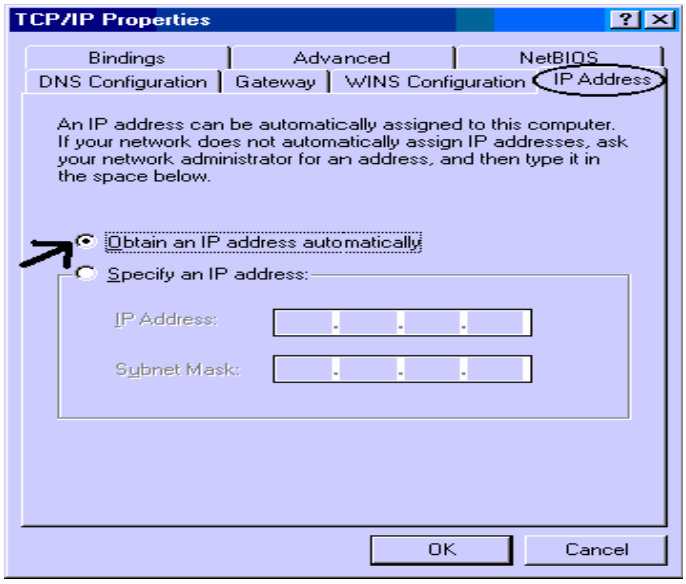

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Configuring PC in Windows 95/98/ME

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.
2. Select **TCP / IP -> NE2000 Compatible**, or the name of your Network Interface Card (NIC) in your PC.
3. Click **Properties**.

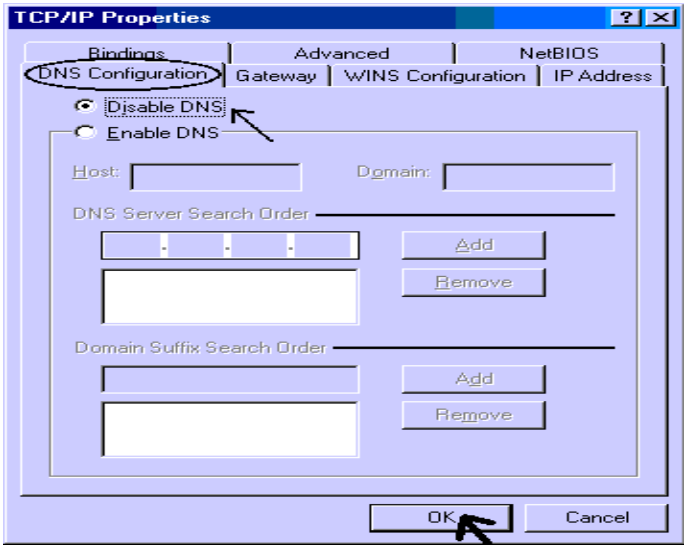


4. Select the **IP Address** tab. In this page, click the **Obtain an IP address automatically** radio button.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

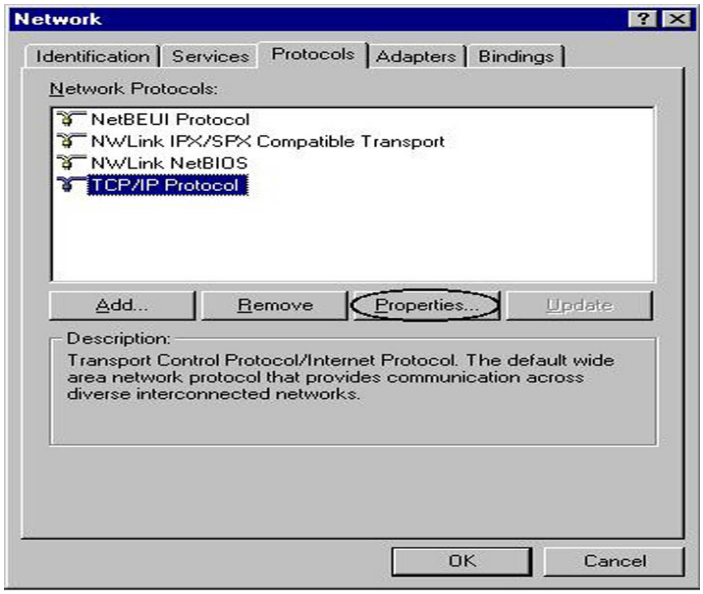
5. Then select the **DNS Configuration** tab.

6. Select the **Disable DNS** radio button and click **OK** to finish the configuration.

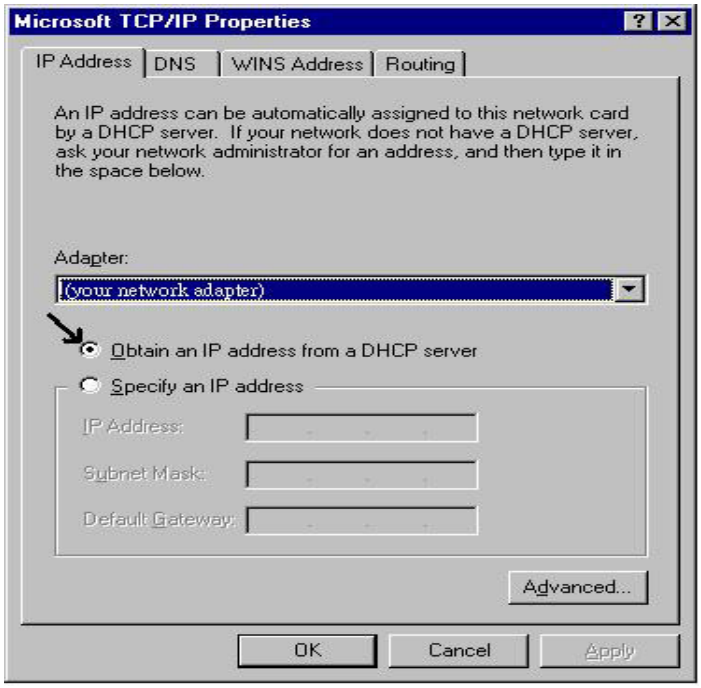


Configuring PC in Windows NT4.0

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Protocols** tab.
2. Select **TCP/IP Protocol** and click **Properties**.



3. Select the **Obtain an IP address from a DHCP server** radio button and click **OK**.


Microsoft TCP/IP Properties
IP Address
DNS
WINS Address
Routing
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Adapter:
(your network adapter)
Obtain an IP address from a DHCP server
Specify an IP address
IP Address:
Subnet Mask:
Default Gateway:
Advanced...
OK
Cancel
Apply

3.2 Factory Default Settings

Before you configure this device, you need to know the following default settings.

1. **Web Configuration**

   Password : <BLANK>
   BLANK means user does not need to input any characters.

2. **Device IP Network settings in LAN site**

   IP Address: 192.168.1.254
   Subnet Mask: 255.255.255.0

3. **ISP setting in WAN site**

   Obtain an IP address automatically

4. **DHCP server**

   DHCP server is enabled.
   IP address pool from IP Address: 192.168.1.100 to IP Address: 192.168.1.199

3.2.1 Password

The password is left blank as the default setting. When configuring your router with Web browser, just click **"OK"**, and then you are logged in for the first time. It is recommended that you set a password for security and management purpose. BIPAC 6600 maintains the password only. It means BIPAC 6600 only checks the password even you enter characters in the User Name field.

If you ever forget the password to log in, you may press the RESET button up to 2 seconds to restore the factory default settings.

3.2.2 LAN and WAN Port Addresses

The parameters of LAN and WAN ports are pre-set in the factory. The default values are shown below.

LAN Port		WAN Port
IP address	192.168.1.254	Obtain an IP address automatically. ISP assigns this IP address.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199 (Actually, it can supports up to 253 users.)	

3.3 Information from ISP

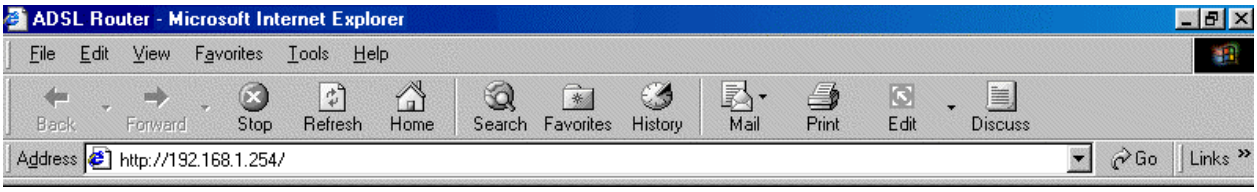
Before you start configuring this device, you have to check with your ISP what kind of service is provided such as PPPoE, Fixed IP, and obtain an IP address automatically.

Gather the information as illustrated in the following table and keep it for reference.

PPPoE	Username, Password, Service Name, Domain Name System (DNS) IP address (it can be automatically assigned from ISP or be set fixed)
Fixed IP	IP address, Subnet mask, Gateway address, Domain Name System (DNS) IP address (it is fixed IP address)
Obtain an IP Address Automatically	Domain Name System (DNS) IP address (it can be automatically assigned from ISP or be set fixed)

3.4 Configuring with Web Browser

Open the web browser, enter the local port IP address of the Broadband Router, which default at **192.168.1.254**, and click "**Go**" to get the login page.


ADSL Router - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address http://192.168.1.254/
Go Links

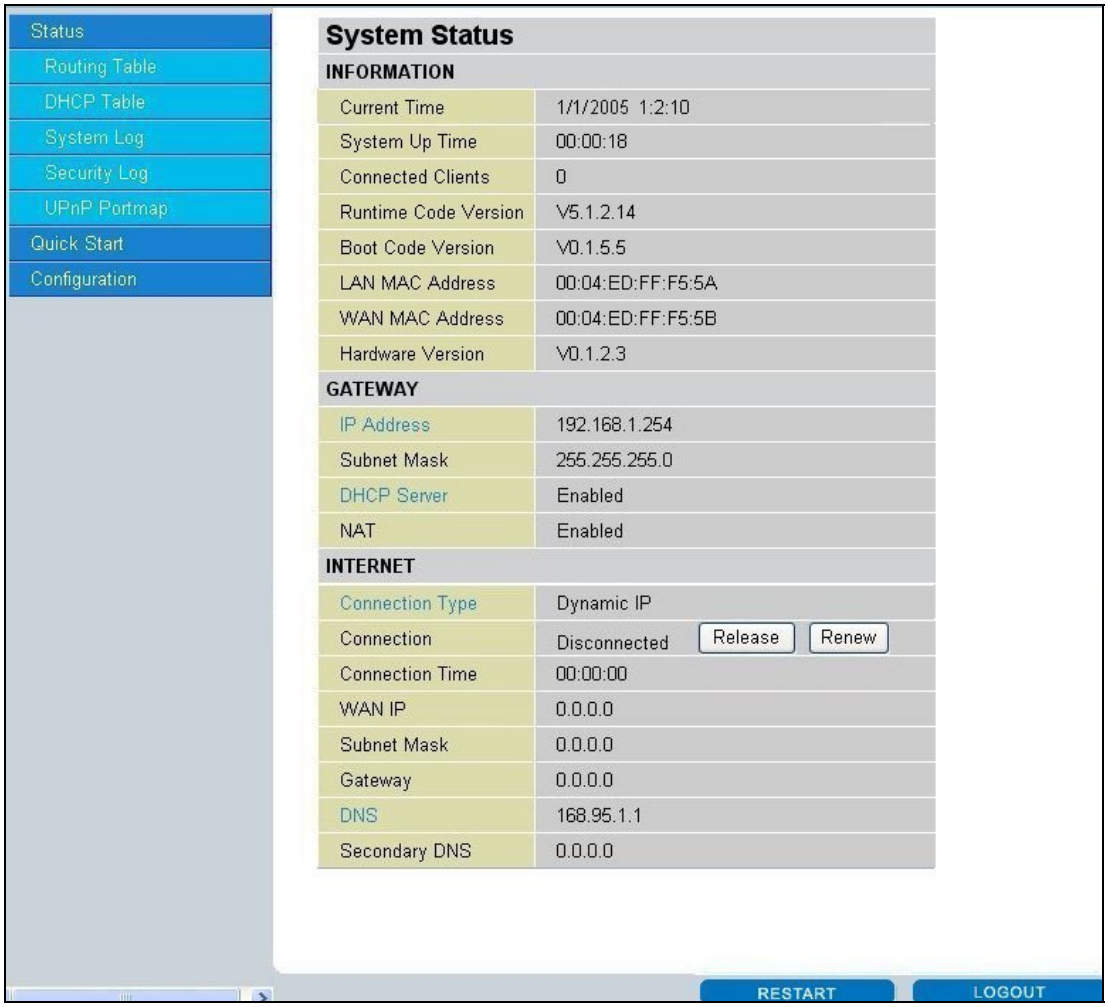
No user name is required. The default password is left blank. If you have set a password, enter that and click **"OK"** to continue.

At the configuration homepage, the left navigation pane where bookmarks are provided links you directly to the desired setup page, including:

- **Status** (Routing Table, DHCP Table, System Log, Security Log, UPnP Portmap)
- **Quick Start**
- **Configuration** (LAN, WAN, System, Firewall, Virtual Server, Advanced)

3.4.1 Status

This section provides useful information for users to review the system status of device. The Status includes hardware version, Gateway information, LAN and WAN IP, and Port status, etc.

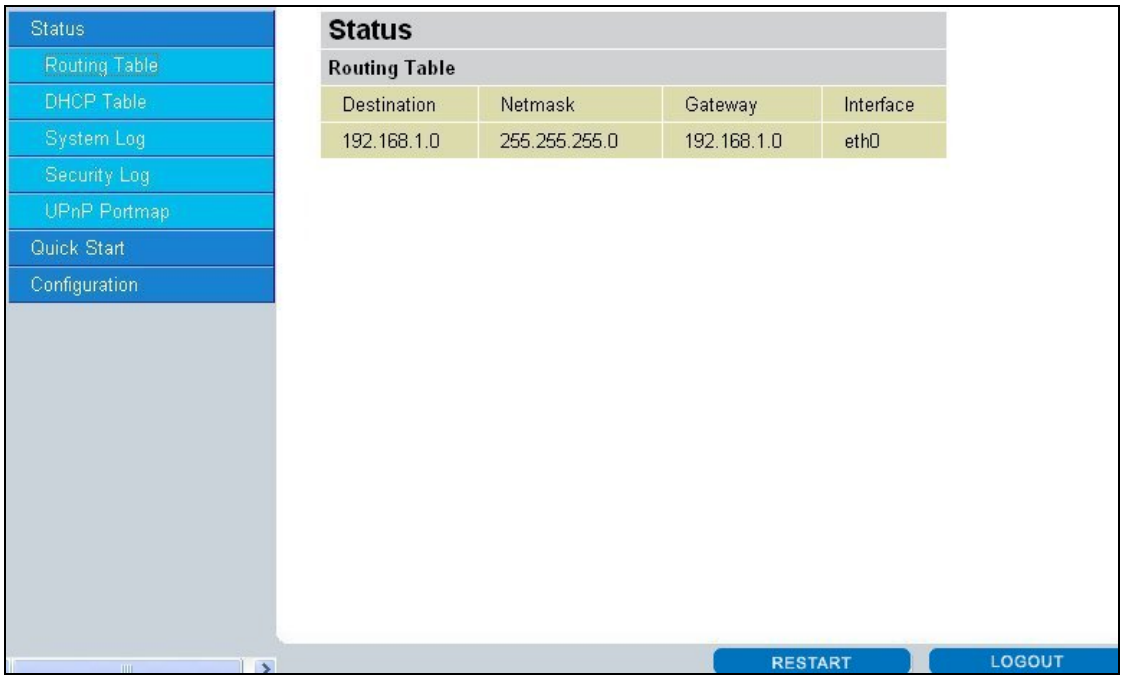


LOGOUT: Logout the device when you finish configuring the router.

RESTART: In case the router stops responding correctly or in some other way stops functioning, you can perform the reboot. Your setting won't be changed. Performing the reboot, click on the **Restart** button.

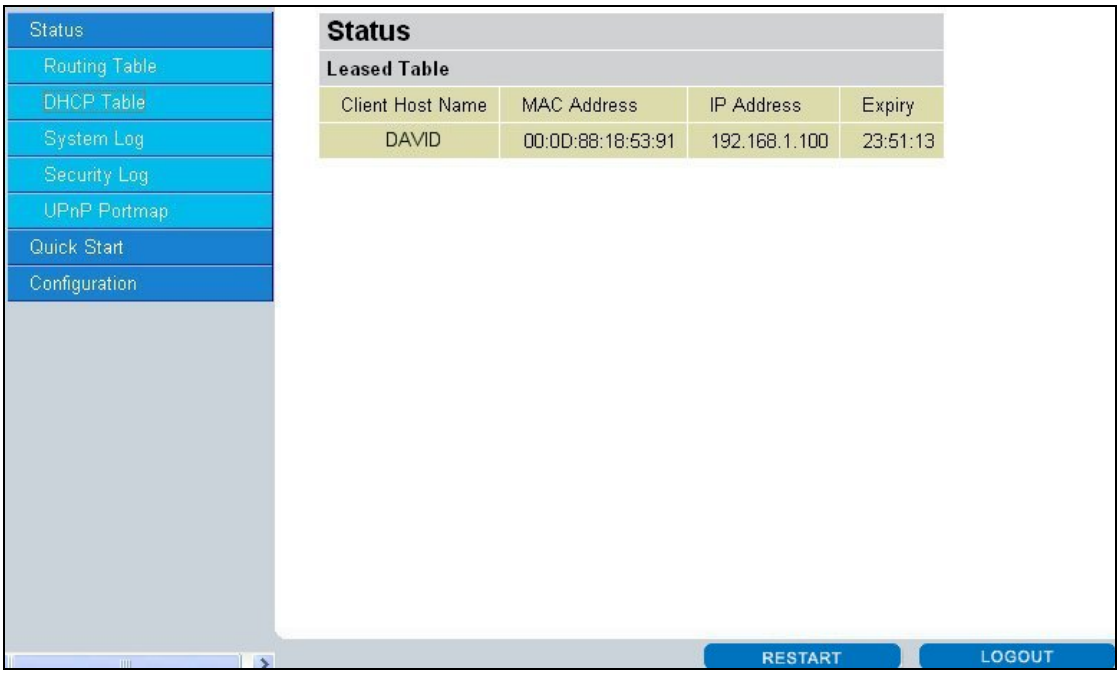
3.4.1.1 Routing Table

Display the current routing paths of BIPAC 6600



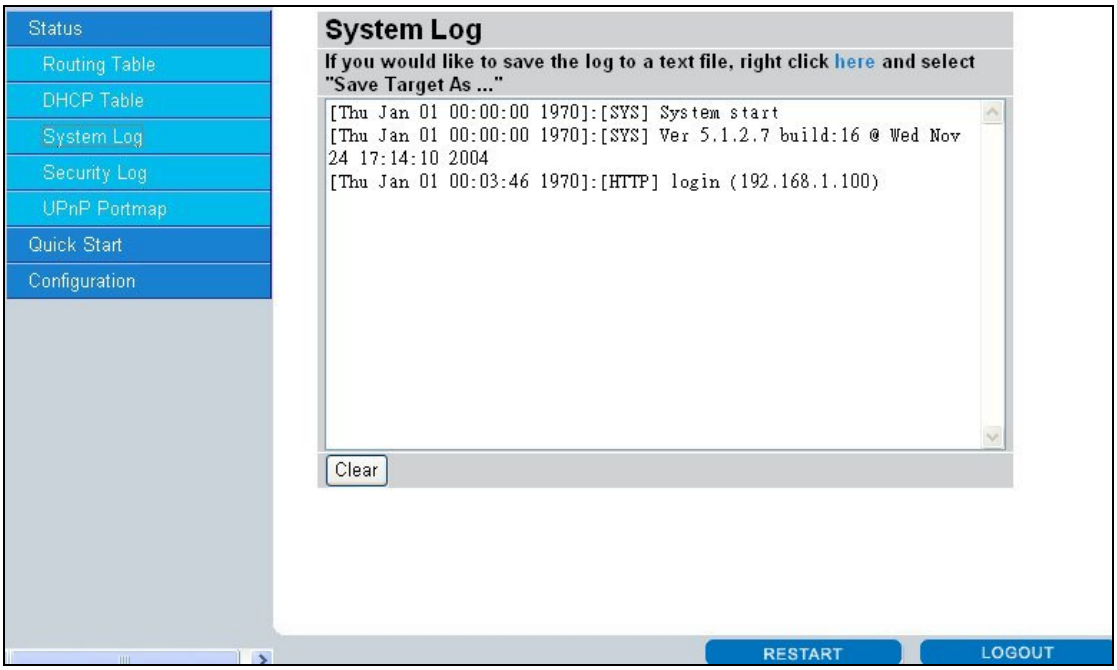
3.4.1.2 DHCP Table

If you enable the DHCP server function of this device, you can see the assigned IP addresses and their associated MAC addresses from this table.



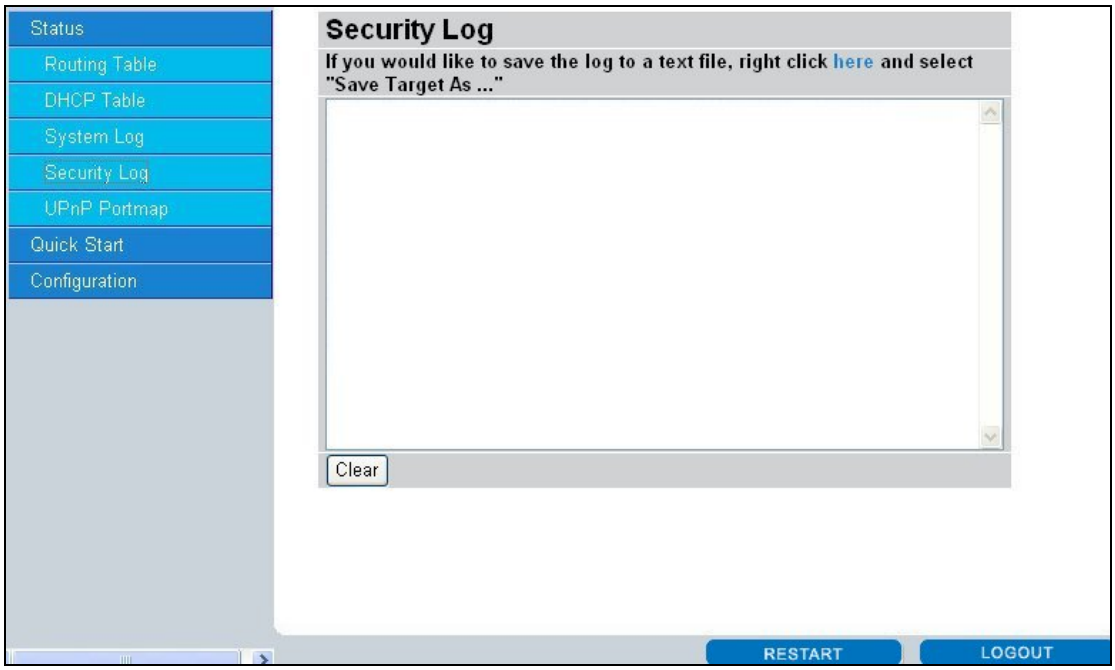
3.4.1.3 System Log

Display the system logs cumulated till the present time. You can trace the historical information through this function. You can also save the log into a text file by clicking “here” and select “Save Target As…”.


Status
Routing Table
DHCP Table
System Log
Security Log
UPnP Portmap
Quick Start
Configuration
System Log
If you would like to save the log to a text file, right click here and select "Save Target As ..."
[Thu Jan 01 00:00:00 1970]:[SYS] System start
[Thu Jan 01 00:00:00 1970]:[SYS] Ver 5.1.2.7 build:16 @ Wed Nov 24 17:14:10 2004
[Thu Jan 01 00:03:46 1970]:[HTTP] login (192.168.1.100)
Clear
RESTART
LOGOUT

3.4.1.4 Security Log

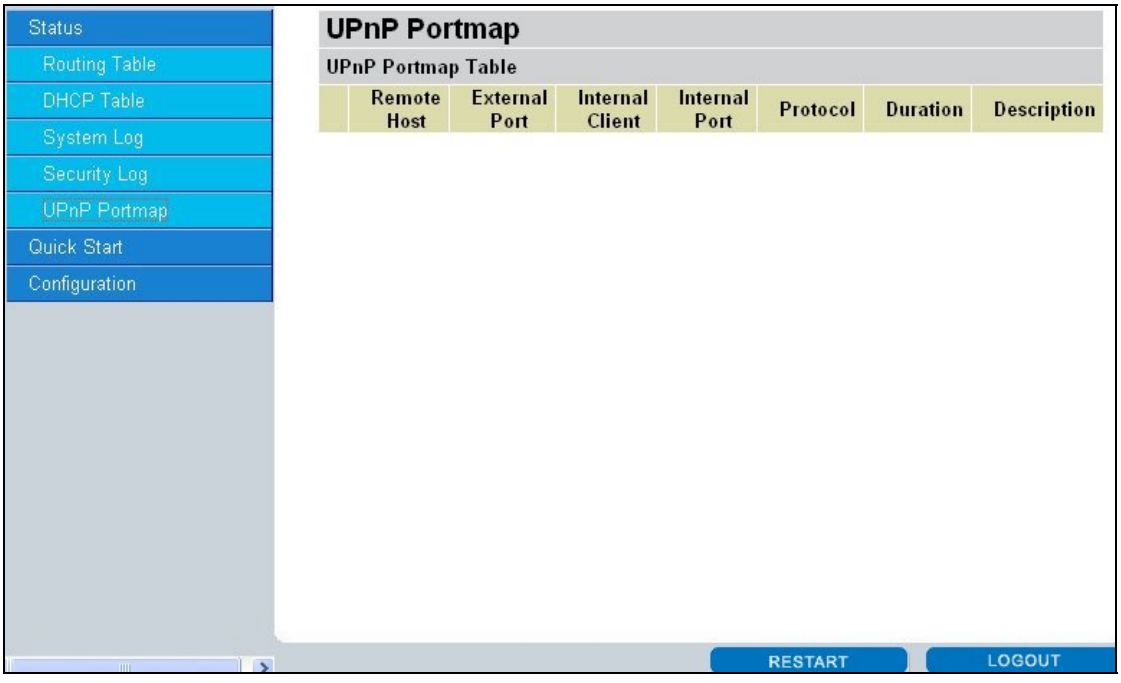
Display the information of security logs. If hacker attacks your sever, he will be isolated by the firewall function and the router will record related information. Hence, you know where the hacker comes from.



3.4.1.5 UPnP Portmap

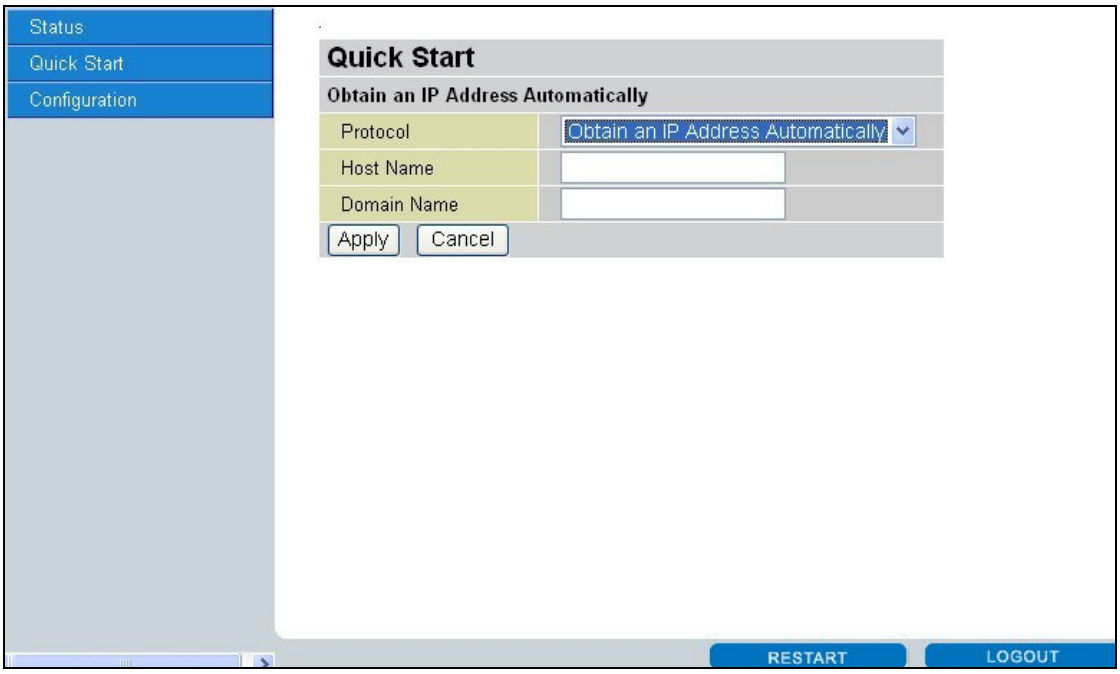
Universal Plug and Play (UPnP) is architecture for pervasive peer-to-peer network connectivity of PCs and intelligent devices or appliances, particularly within the home. UPnP builds on Internet standards and technologies, such as TCP/IP, HTTP, and XML, to enable these devices to automatically connect with one another and work together to make networking - particularly home networking - possible for more people.

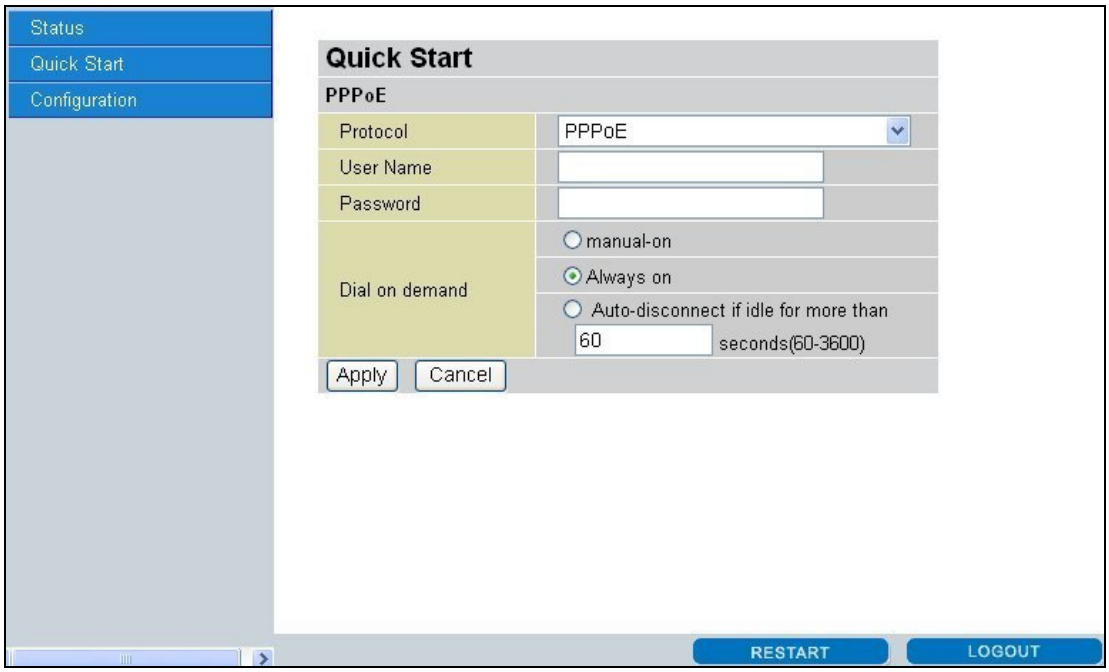
The UPnP aware applications will discover that they are behind a NAT router, learn the external IP address and configure port mappings on the router to forward packets from the external ports of the router to the internal ports used by the application.

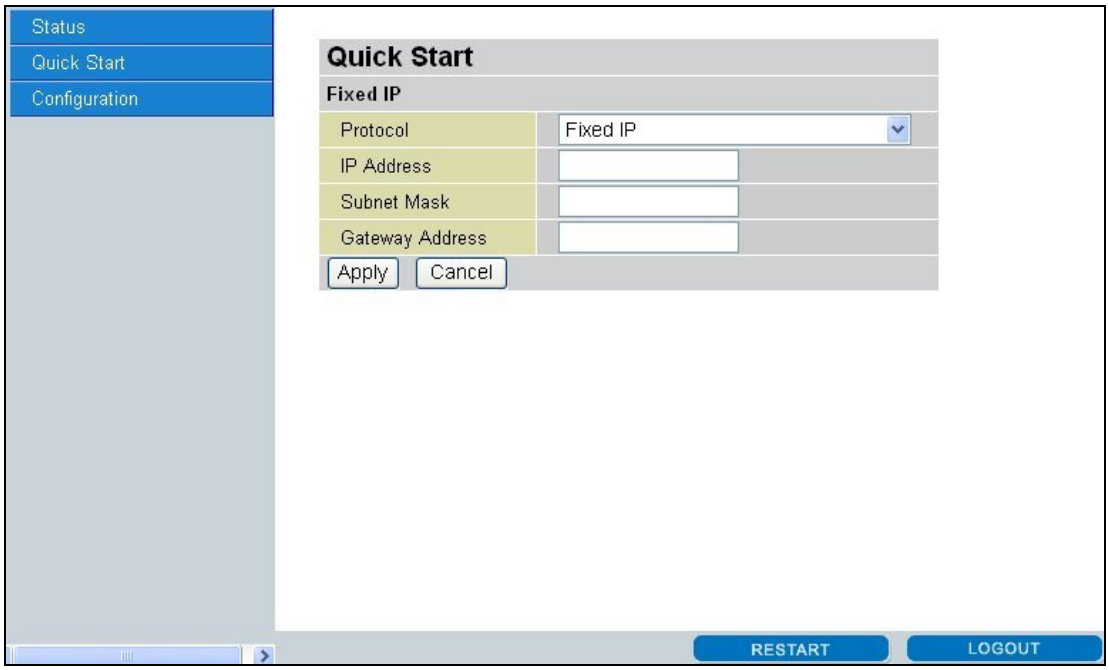


3.4.2 Quick Start

If you use this device to access the Internet through the ISP, this web page is enough for you to configure this router and access the Internet without a problem. Please check **Chapter 3.3** (*Information from the ISP)*, then enter the proper values into this web page, click the **Apply** button to save all of the configuration parameters to FLASH. Then you may check the Status web page to check whether the router is connected to the ISP or not. In most cases, you can access the Internet immediately. If not, please refer to the sections below for more information.







3.4.3 Configuration

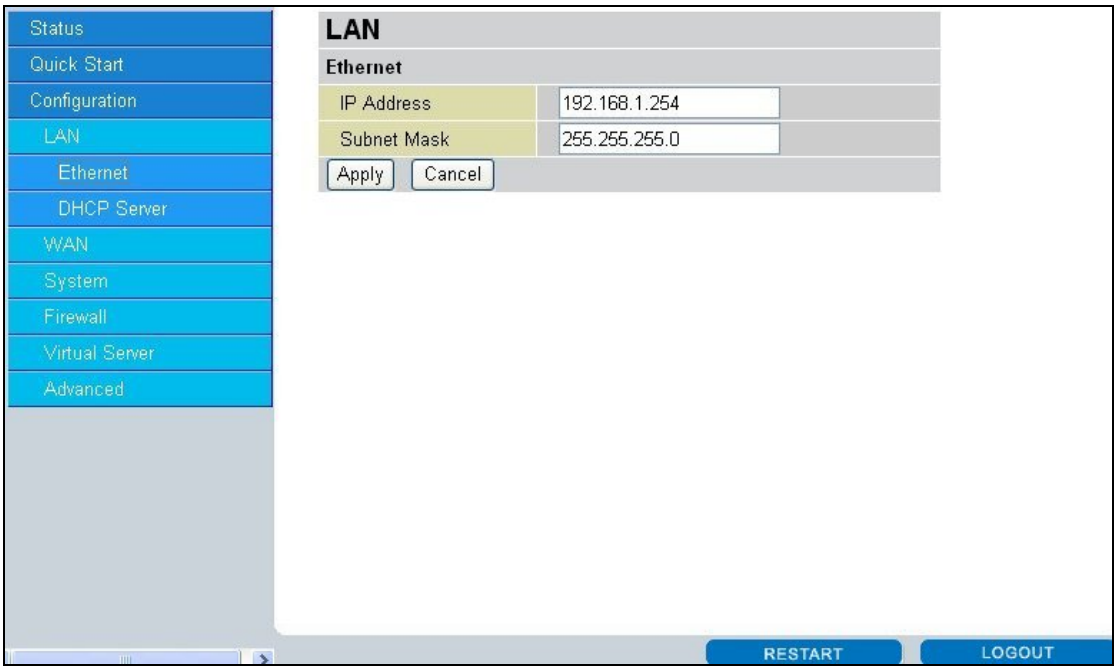
When you click this item, you get following sub-items to configure BIPAC 6600.

LAN, WAN, System, Firewall, Virtual Server, and Advanced

3.4.3.1 LAN

This screen contains settings for LAN interface attached to the LAN port.

3.4.3.1.1 Ethernet

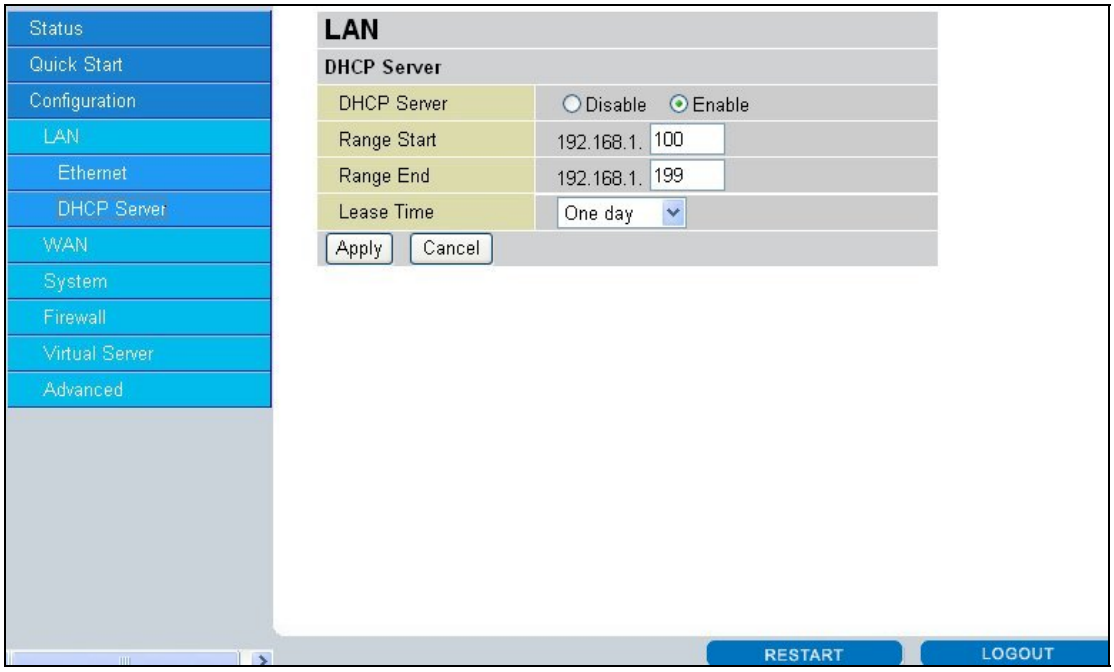


IP Address: Default at 192.168.1.254.

This is the device IP address in LAN site. If you plan to change it to another IP address to a different range of IP subnet. Please make sure your PC is also located at the same IP subnet. Otherwise, you may not be able to access the router.

Subnet Mask: Default at 255.255.255.0.

3.4.3.1.2 DHCP Server



DHCP Server: Check DHCP Server "**Enable**" to allow the router distributes IP Addresses, subnet mask and DNS setting to computers. The following fields will be activated. If you check "**Disable**", remember to specify a static IP address, subnet Mask, and DNS setting for each of your local computers. Be careful not to assign the same IP address to different computers.

Range Start: Enter the start address of this local IP network address pool. The pool is a piece of continuous IP address segment. The default value is 192.168.1.100.

Range End: Enter the last address of this local IP network address pool that you want the DHCP server to assign IP addresses to. The default value is 192.168.1.199.

With this case, the DHCP pool is from 192.168.1.100 to 192.168.1.199. Therefore, the local computer will get an IP address located at this range randomly.

Lease Time: Set the lease time you required.

3.4.3.2 WAN

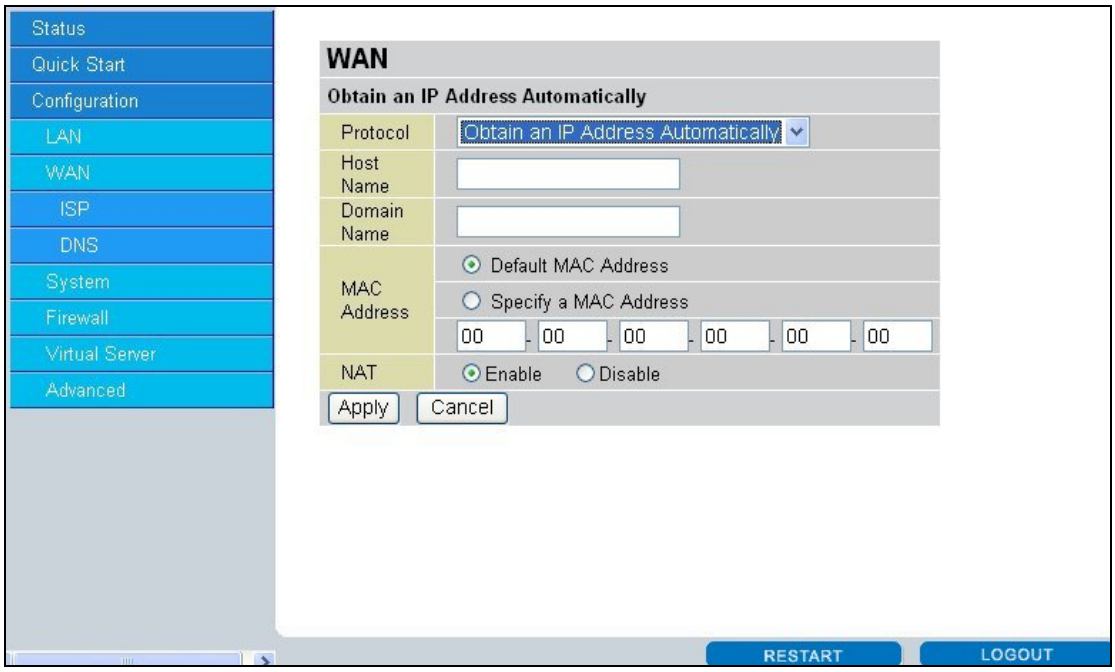
The screens below contain settings for the WAN interface toward Internet.

There are three kinds of protocols provided — Obtain an IP Address Automatically (DHCP Client), PPPoE, and Fixed IP — for the device to have a public IP address and then to access Internet. You have to check with your ISP about which way is adopted.

3.4.3.2.1 ISP

Obtain an IP Address Automatically

Configure this WAN interface to use DHCP client protocol to get an IP address from ISP automatically. In other words, the ISP provides an IP address to the router dynamically when logon.



Host Name: Enter the host name provided by your ISP. The maximum input is **20** alphanumeric characters (case sensitive).

Domain Name: Enter the domain name provided by your ISP. The maximum input is **20** alphanumeric characters (case sensitive).

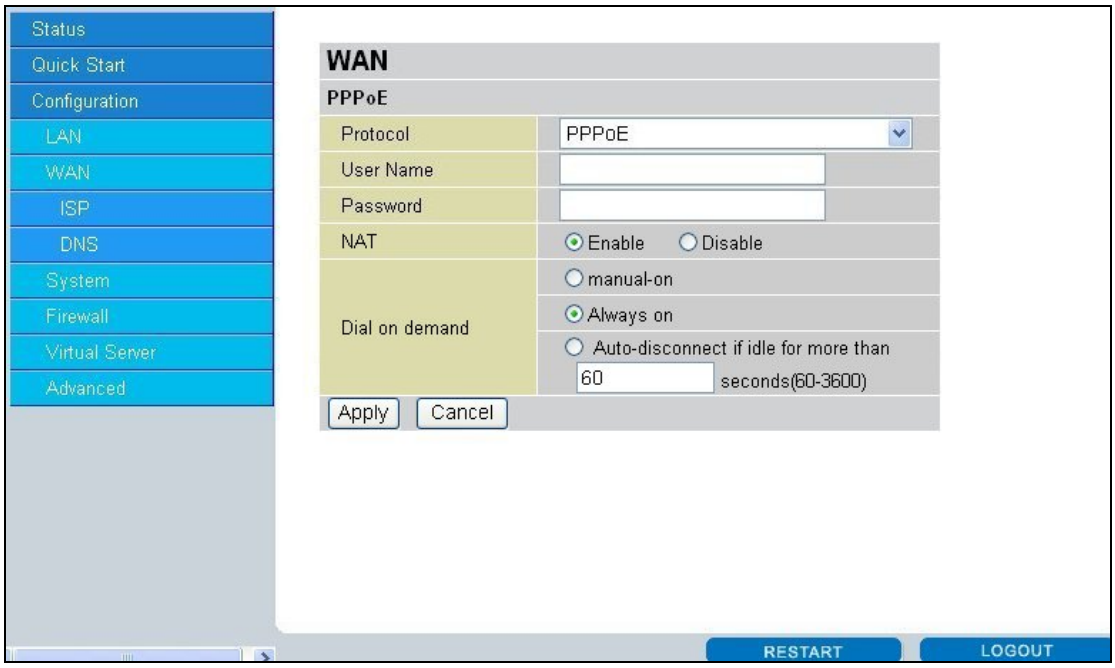
MAC Address: Specify the MAC address if your ISP needs it. The Default MAC address is router's MAC address.

NAT: The NAT feature allows multiple users to access Internet through a single IP account, sharing the single IP address from ISP. If users in the LAN site have public IP addresses and can access Internet directly, the NAT function can be disabled.

*The **Router Name**, **Domain Name** and **MAC Address** fields are needed for some ISPs. Please check it with your ISP. If you and your ISP do not know it, please leave it as default.*

PPPoE

PPPoE (PPP over Ethernet) is known as a dial-up DSL or cable service. It is designed to integrate the broadband services into the current widely deployed, easy-to-use, and low-cost dial-up-access networking infrastructure. Therefore, users can get greater access speed without changing the operation concept, sharing the same ISP account and paying for one access account. No PPPoE client software is required for local computer if you select this configuration.



Username: Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).

NAT: The NAT feature allows multiple users to access Internet through a single IP account, sharing the single IP address. If users in the LAN site have public IP addresses and can access Internet directly, the NAT function can be disabled.

Manual-on: Check this button to establish your WAN connection manually by clicking "**Release**" in "**3.4.1 Status** " section.

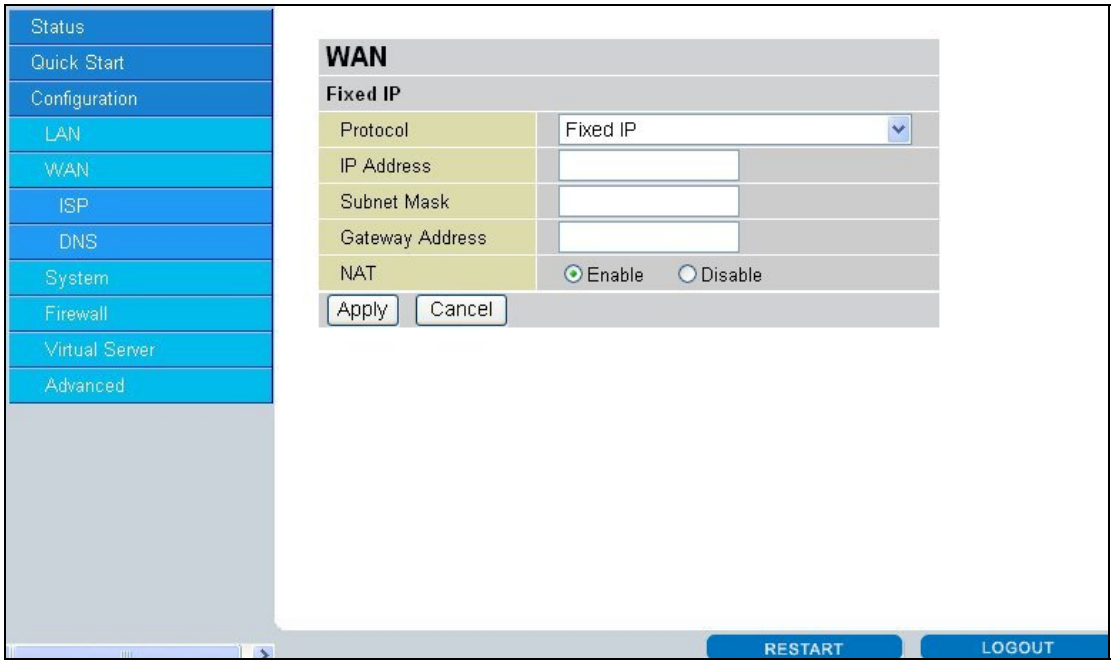
Always on: Check this radio button if you want to establish a PPPoE session when starting up the device. Please note that when you select this function, the device will not automatically re-establish the PPPoE session when disconnected by ISP.

Auto-disconnect if idle for more than ☐ minutes: Check this radio button if you want to establish a PPPoE session only when there is a packet requesting for going out to the Internet. The device will be auto-disconnected when there is no activity on the line for a predetermined period of time. You can input any number from **0 to 999**. The default value is **5** minutes.

After all of the settings are done, you need to click on "Apply" button to save them permanently.

Fixed IP

Configure this WAN interface with a specific IP address. This IP address should be given from ISP directly.



IP Address: Enter the information provided by your ISP.

Subnet Mask: Enter the information provided by your ISP.

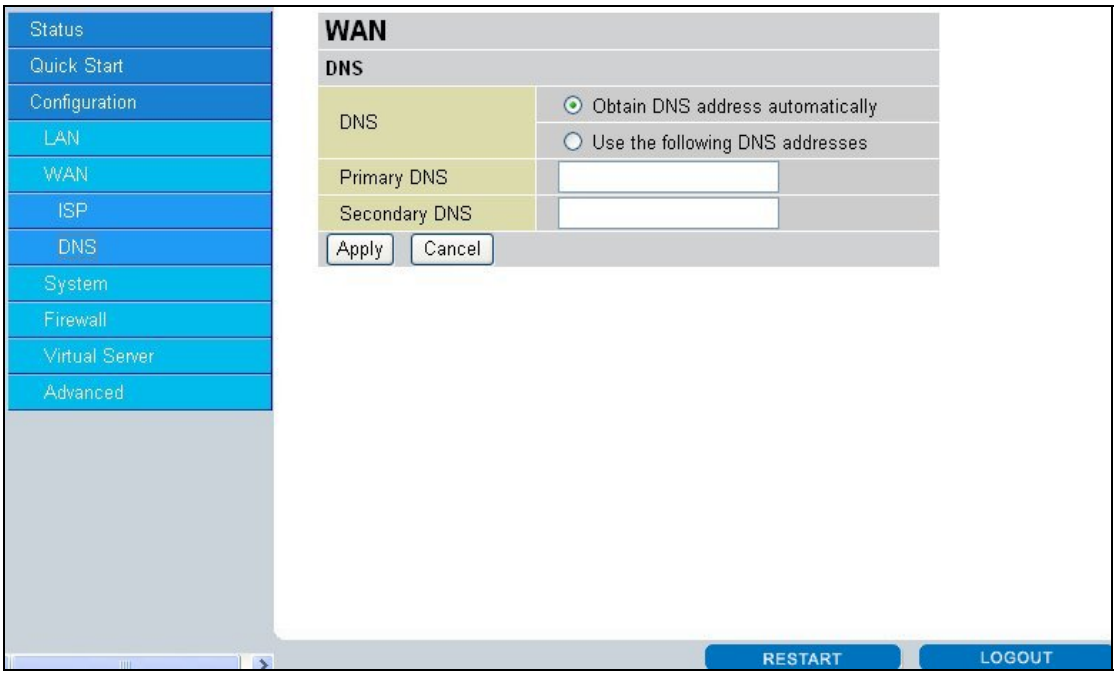
Gateway Address: Enter the information provided by your ISP.

NAT: The NAT feature allows multiple users to access Internet through a single IP account, sharing the single IP address. If users in the LAN site have public IP addresses and can access Internet directly, the NAT function can be disabled.

3.4.3.2.2 DNS

A Domain Name System (DNS) contains a mapping table for domain name and IP address. In the Internet, every host has a unique and friendly name such as www.yahoo.com and IP

address. The IP address is very hard to remember, so that you may just enter the friendly name www.yahoo.com and DNS converts it to its equivalent IP address.



You can obtain Domain Name System (DNS) IP address automatically if ISP provides it when you logon. This **Obtain DNS address automatically** selection is set as default when you choose Obtain an IP Address Automatically, PPPoE, or Fixed IP as your WAN protocol.

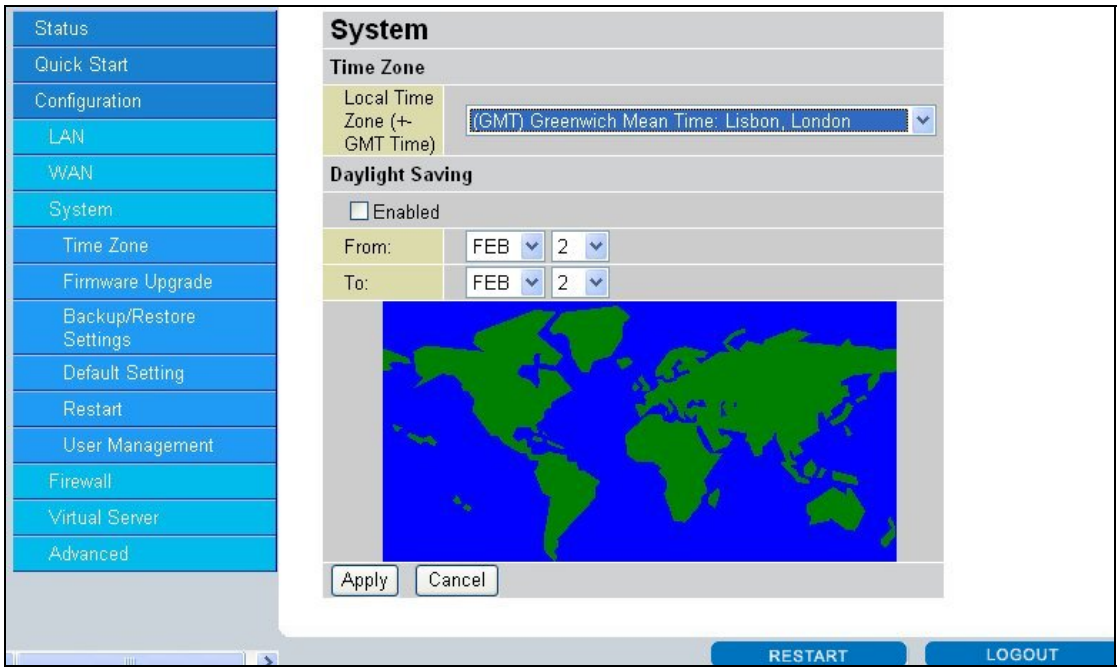
Or your ISP may provide you with an IP address of DNS. If this is the case, you must enter the DNS IP address. Moreover, if you set Fixed IP as your ISP protocol, you can only enter the DNS IP Address instead of obtaining the address automatically.

3.4.3.3 System

There are five items under the **System** section: Time Zone, Firmware Upgrade, Backup/Restore Settings, Default Settings, Restart and User Management.

3.4.3.3.1 Time Zone

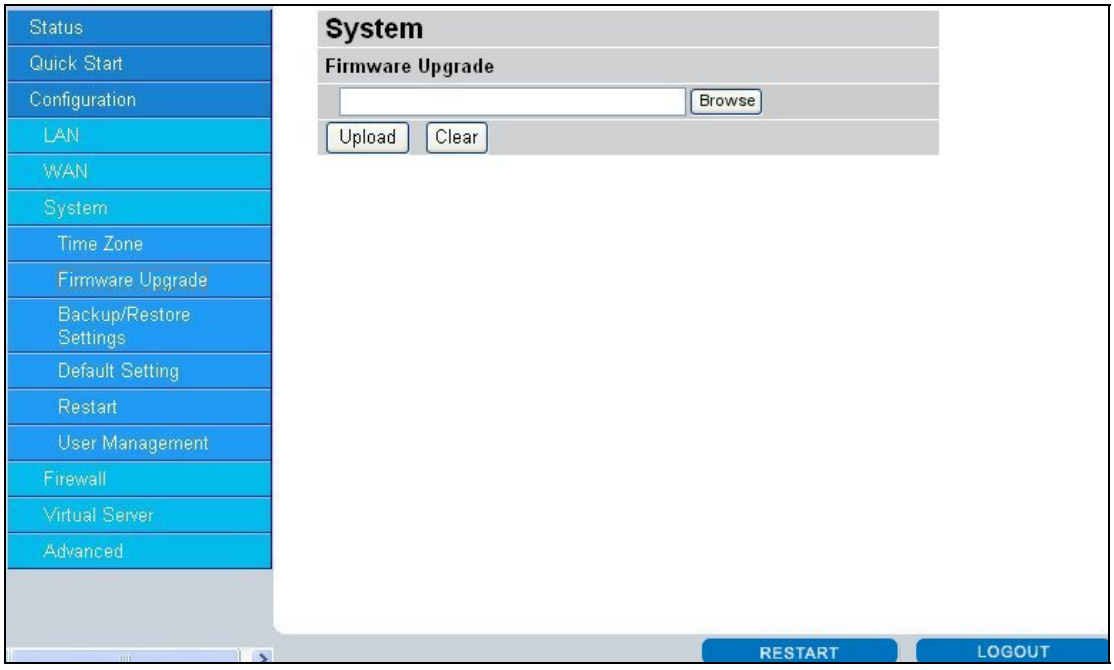
BIPAC 6600 does not have a real time clock on board; instead, it uses the simple network time protocol (SNTP) to get the current time from the SNTP server in outside network. Please choose your local time zone and click Submit. You will get the correct time information after you really establish a connection to Internet. The current time of selected time zone will be shown in the Status – System window.



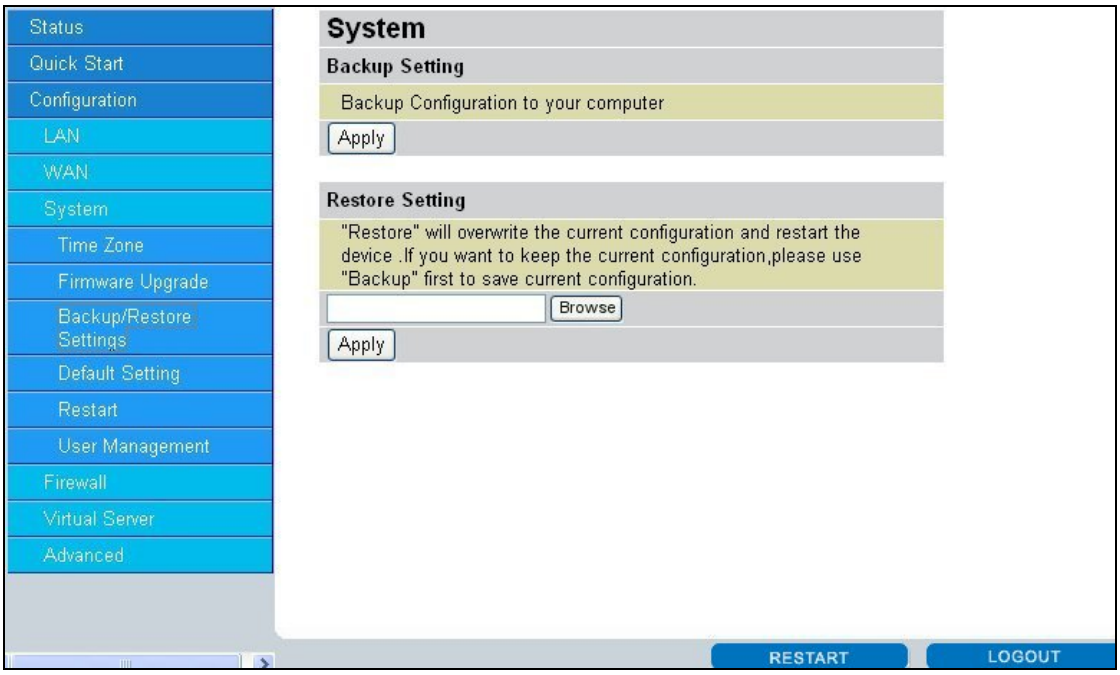
Daylight Saving: It is optional for different time zone area.

3.4.3.3.2 Firmware Upgrade

To upgrade the firmware of BIPAC 6600, you should download or copy the firmware to your local environment first. Press the **"Browse…"** button to specify the path of the firmware file. Then, click **"Upgrade"** to start upgrading. When the procedure is completed, BIPAC 6600 will reset automatically to make the new firmware work.



3.4.3.3.3 Backup/Restore Settings

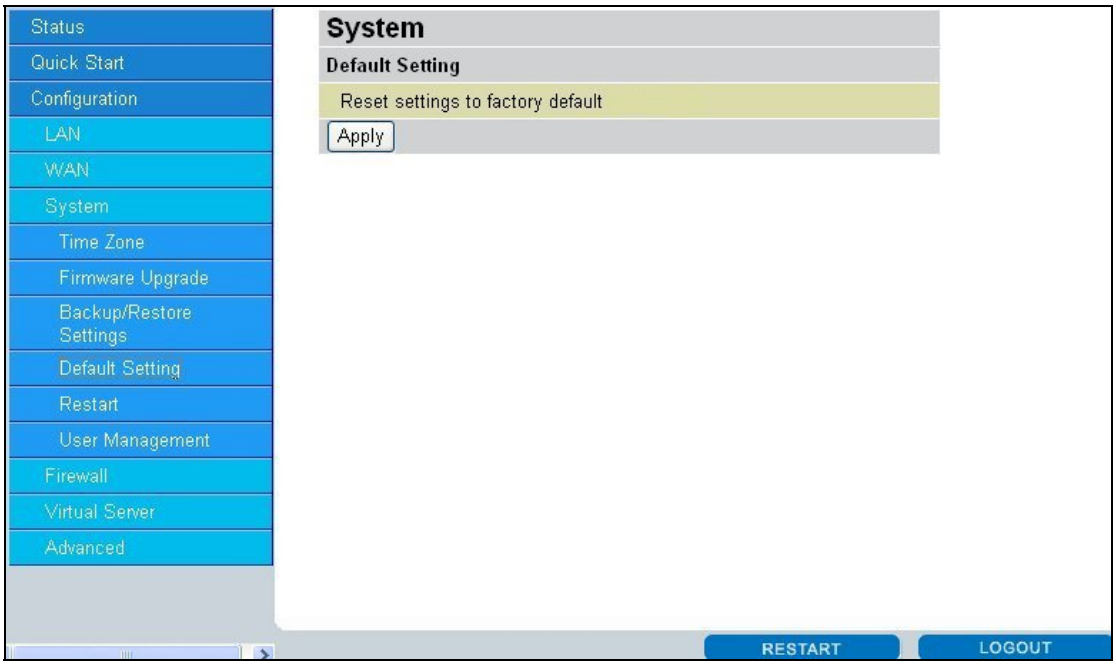


Backup Setting: Backup configuration to your computer.

Restore Setting: "Restore" will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "**Backup**" first to save current configuration.

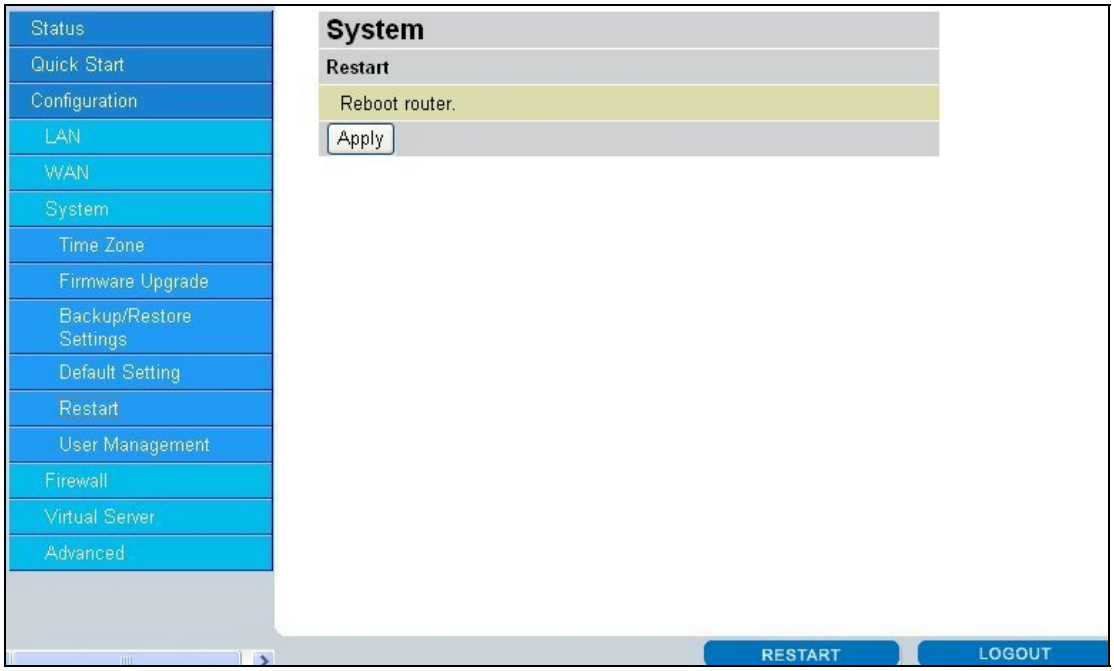
3.4.3.3.4 Default Setting

If for any reason, you have to reset this router back to factory default settings, be careful that the current settings will be lost and the settings are reset back to its default value. The factory default values is detailed in the ***section 3.2 ''Factory Default Settings''*.**

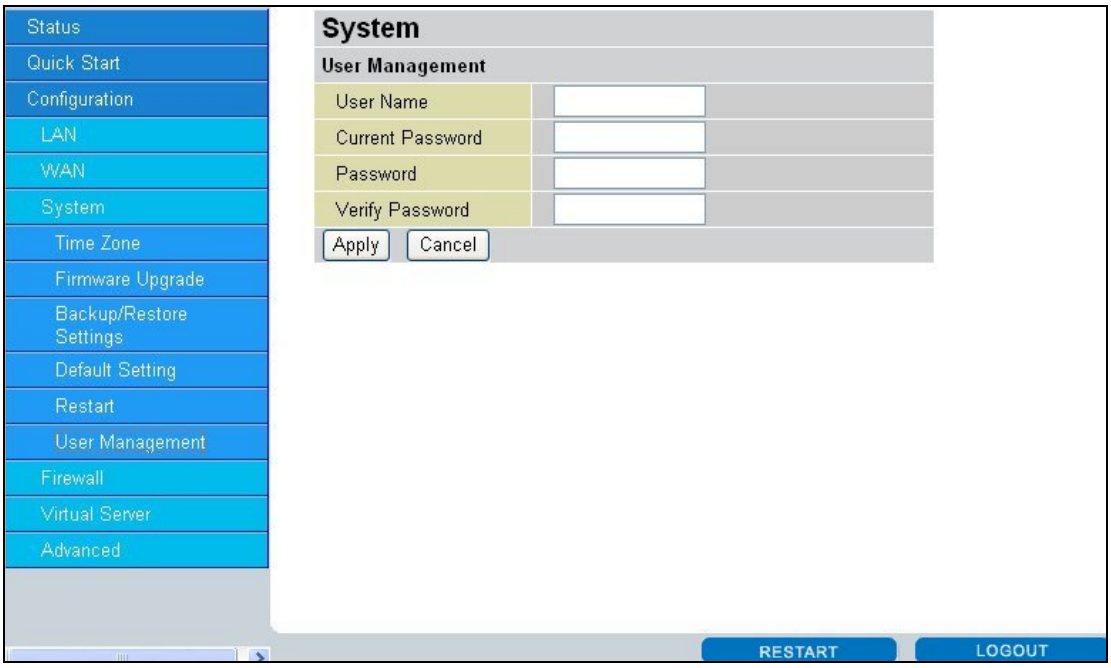


3.4.3.3.5 Restart

In case the router stops responding correctly or in some other way stops functioning, you can perform the restart. Your setting won't be changed. Performing the restart, click on the **Apply** button.



3.4.3.3.6 User Management

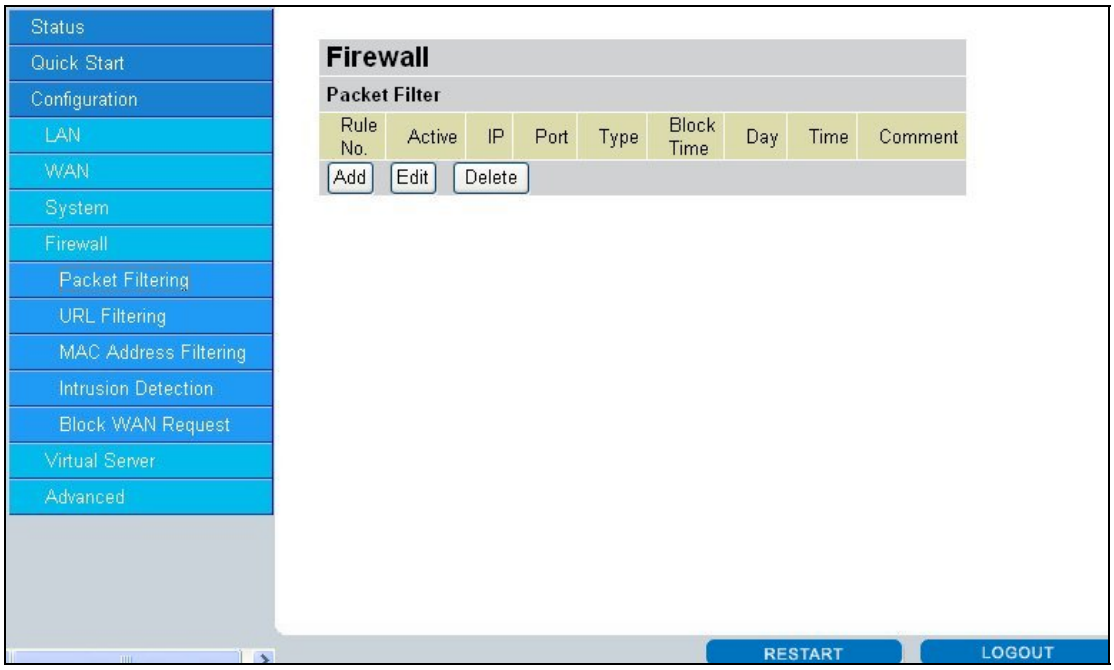


3.4.3.4 Firewall

User can decide to enable this firewall function including Packet Filtering, URL Filtering, MAC Address Filtering, Intrusion Detection, and Block WAN Request features for better security control or not. But be noted, it wastes network processor computation power. The performance will be lower about 10% to 15%.

3.4.3.4.1 Packet Filtering

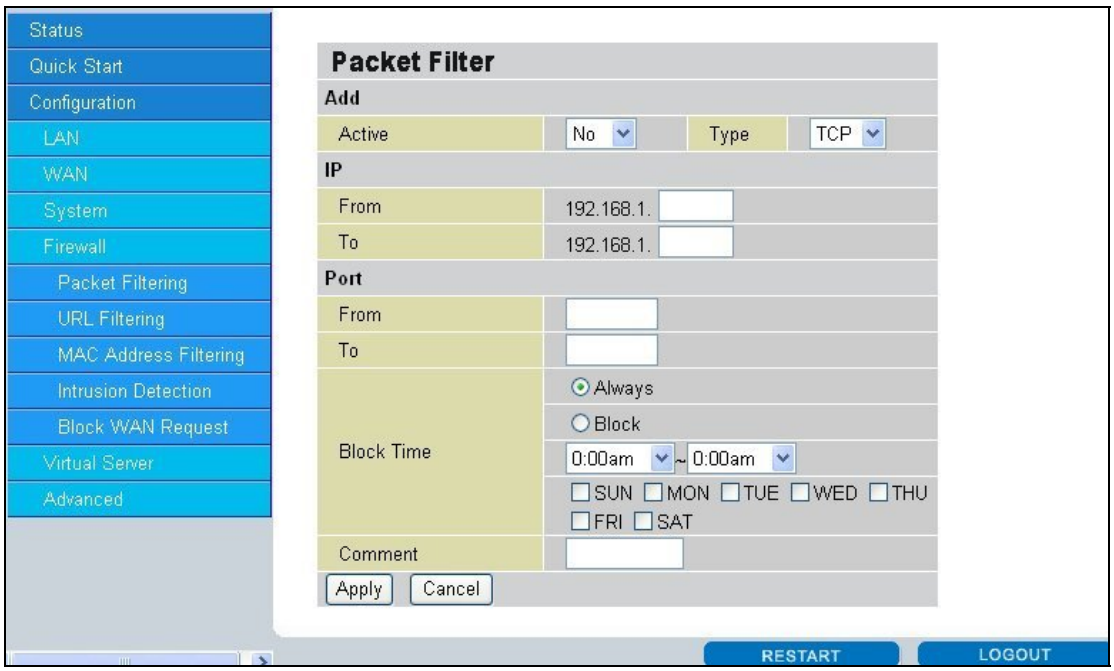
Packet filtering function enables you to configure your router to check specified internal/external user (**IP address**) from Internet access, or you can disable specific service request (**Port number**) to/from Internet. This configuration program allows you to set up different filter rules up to 10 for different users based on their IP addresses or their network Port number. The relationship among all filters is **"or"** operation, which means the device checks these different filter rules one by one, stating from the first rule. As long as one of the rules is satisfied, the specified action will be taken.



Add: Click this button to add a new packet filter rule. After click, next figure will appear.

Edit: Check the Rule No. you want to edit. Then, click the “Edit” button.

Delete: Check the Rule No. you want to delete. Then, click the “Delete” button.



Active: Choose “Yes” to enable the rule, or choose “No” to disable the rule.

Type: Specify the packet type (TCP, UDP, or both) that the rule will be applied to. Select **TCP** if you want to scope for the connection-based application service on the remote server using the port number. Or select **UDP** if you want to scope for the connectionless application service on the remote server using the port number.

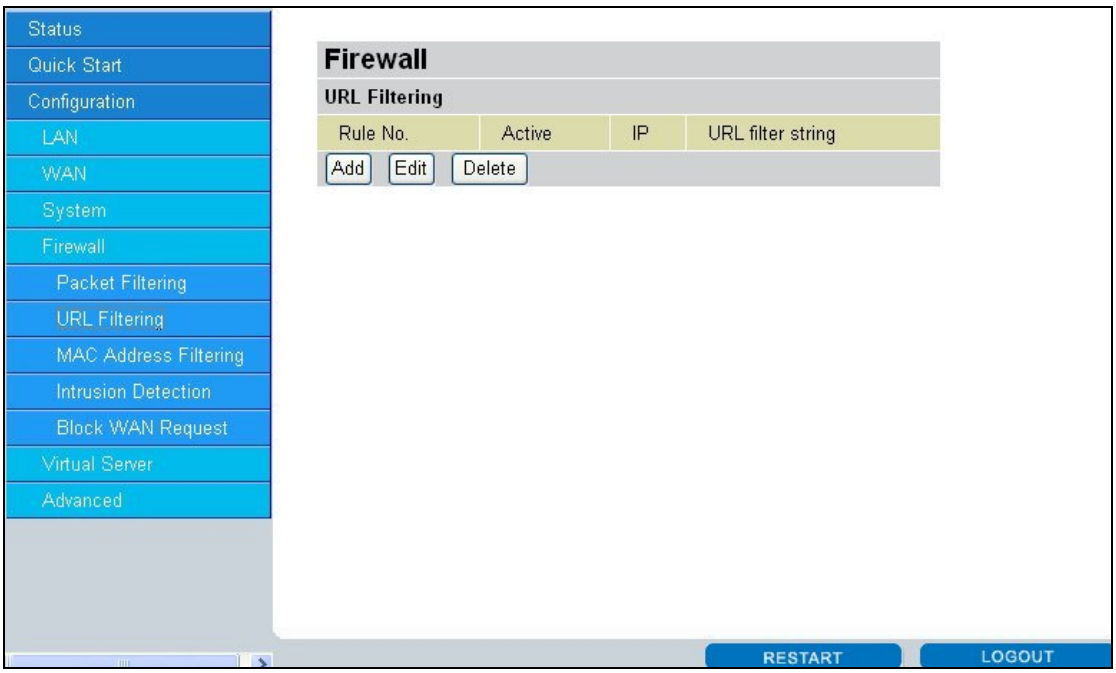
IP Address: Enter the incoming or outgoing packet's source/destination IP address(es).

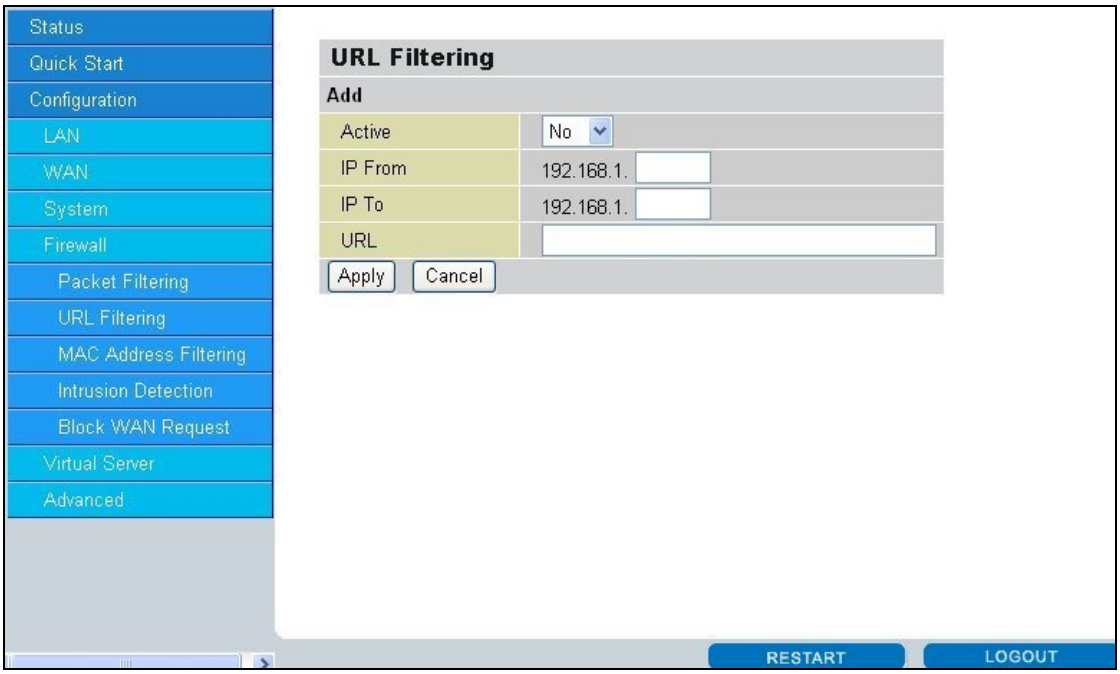
Port: Check the TCP or UDP packet's source/destination port number(s).

If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of filtered private IP range in order to avoid conflicts because you do not know which PC in LAN is assigned to which IP address. The easiest and safest way is that the filtered IP address is assigned to specific PC that is not allowed to access outside resource such as Internet. You configure the filtered IP address manually to this PC, but it is still in the same subnet with the router.

3.4.3.4.2 URL Filtering

URL filtering function enables you to avoid your LAN PCs from accessing some URLs. You must check the Active **"Yes"** radio button to enable the settings.





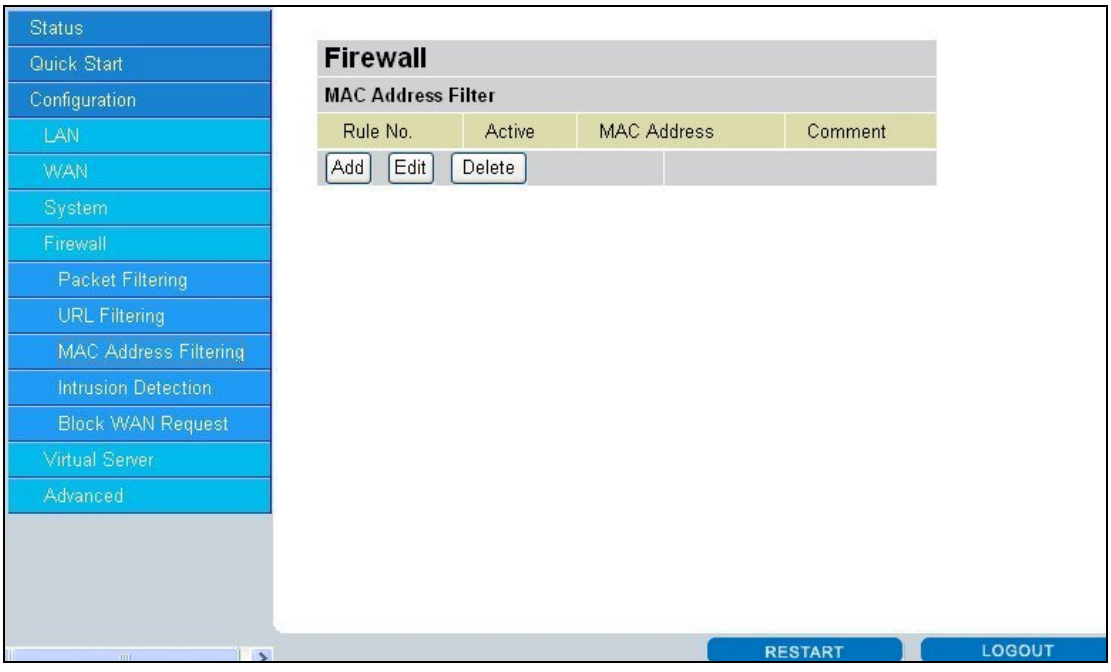
Active: Select "**Yes**" and proceed to the IP address settings.

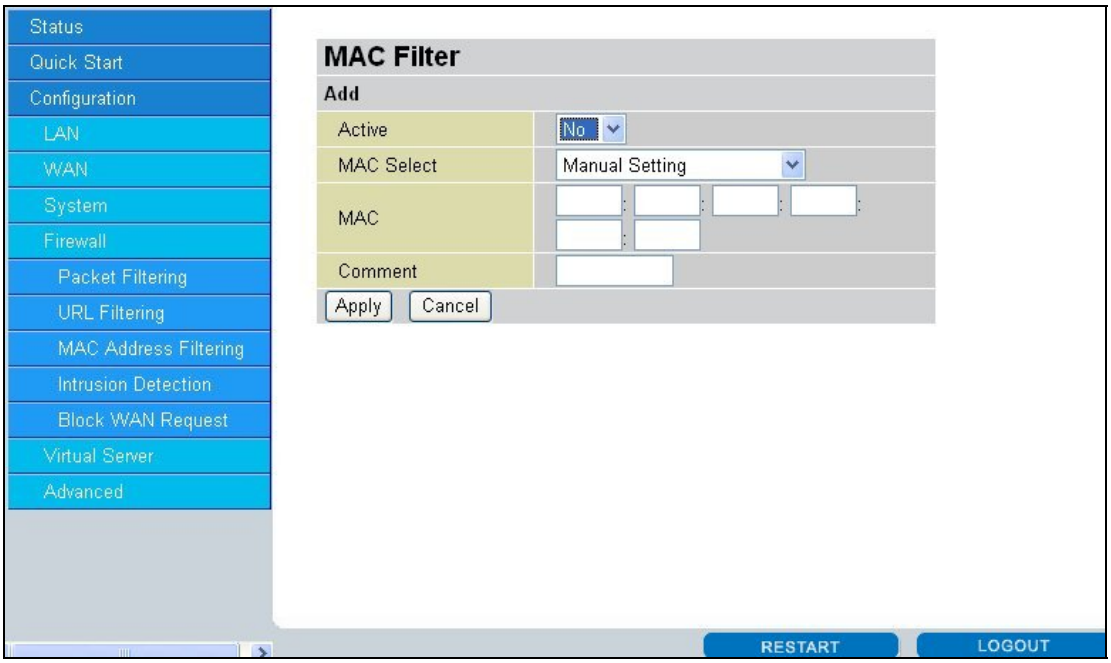
IP: specify the IP address in terms of ranges you want.

URL: enter the URL string you would like to block.

3.4.3.4.3 MAC Address Filtering

MAC address filtering function enables you to configure your router to block specified internal user (**MAC address**) from Internet access.



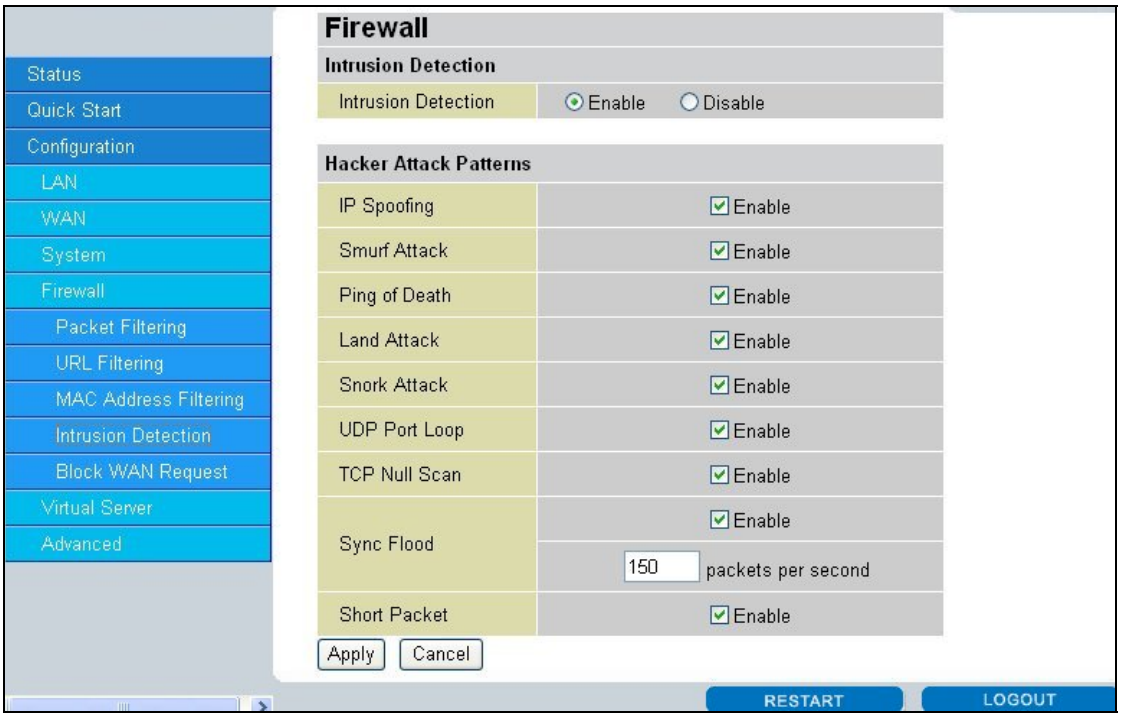


Active: Check **"Yes"** radio button to make the following settings activated.

MAC Select: Select "**Manual Setting**" to enter MAC address and Comment you need, or select default MAC address.

MAC: Enter the MAC address you want to configure. Then, click the "**Apply**" button to save your setting.

3.4.3.4.4 Intrusion Detection

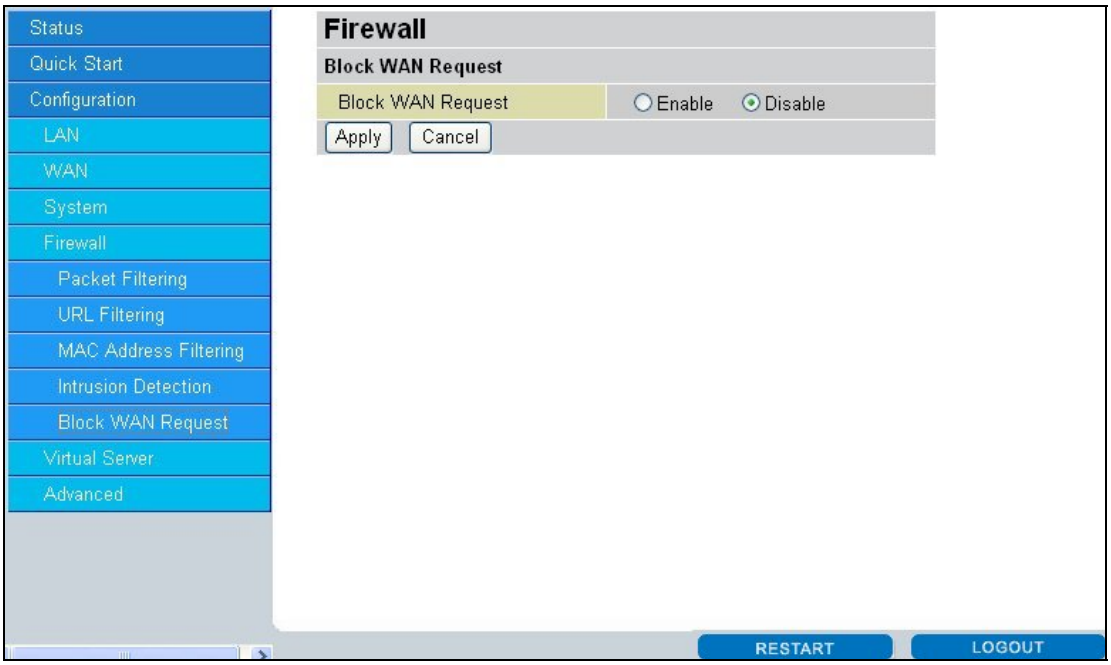


Check “Enable” if you want to detect invader sneak in your computer without permitted .The Broadband Router can automatically detect and block the DoS (Denial of Service) attack if user enables this function. This kind of attack is not to achieve the confidential data of this network; instead, it aims to crush specific equipment or the entire network. If this happens, the users will not be able to access the network resources. There are few samples of hacker patterns implemented as below.

- **IP Spoofing**
- **Smurf Attack (ICMP Echo with x.x.x.0 or x.x.x.255)**
- **Ping of Death (Length > 65535)**
- **Land Attack (Same source / destination IP address)**
- **Snork Attack**
- **UDP port loop**
- **TCP NULL scan**
- **Sync flooding**
- **Short Packet**

3.4.3.4.5 Block WAN Request

Check “**Enable**” if you want to exclude outside PING request from reaching to this router.



3.4.3.5 Virtual Server

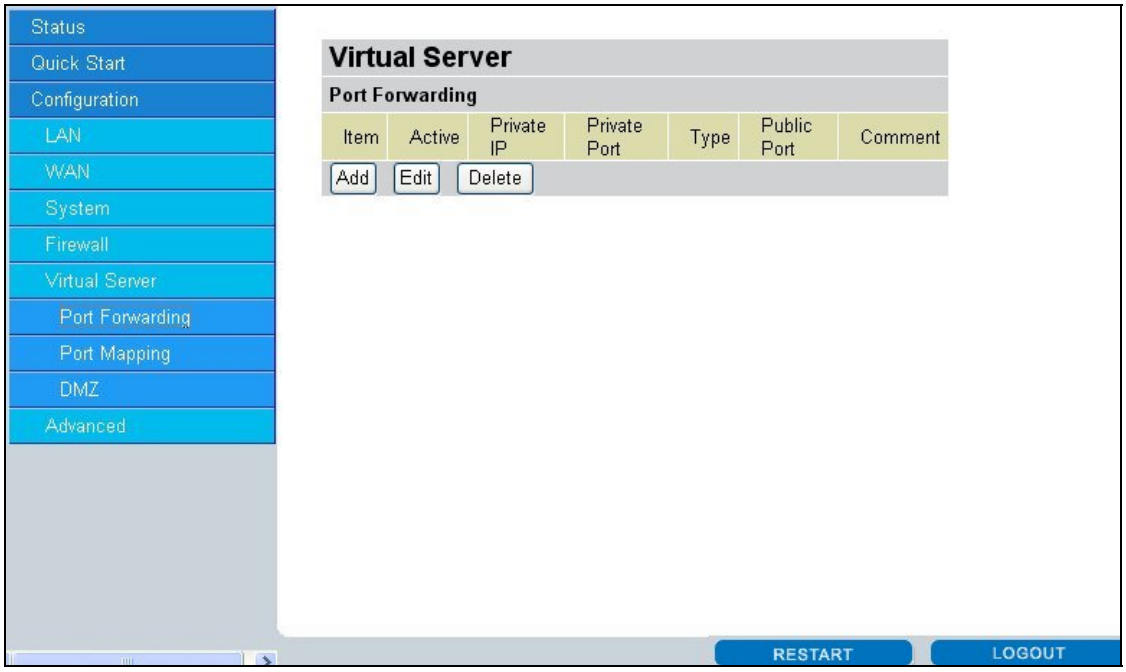
Being a natural Internet firewall, the Broadband Router protects your network from being accessed by outside users. When it needs to allow outside users to access internal servers, e.g. Web server, FTP server, E-mail server or News server, this product can act as a virtual server. You can set up a local

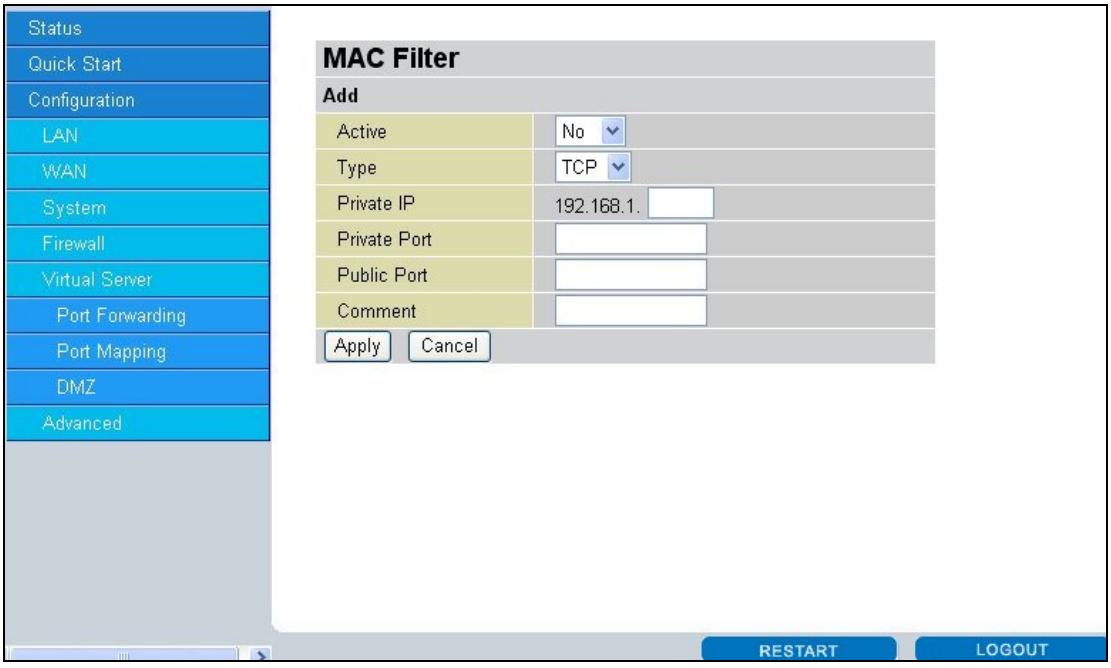
server with specific port number that stands for the service, e.g. Web (80), FTP (21), Telnet (23), SMTP (25), POP3 (110), DNS (53), ECHO (7), NNTP (119). When an incoming access request to the router for specified port is received, it will be forwarded to the corresponding internal server.

For example, if you set the Public Port number 21 (FTP) to be mapped to the IP Address 192.168.1.100, then all the ftp requests from outside users will be forwarded to the local server with IP address of 192.168.1.100.

Here the Router provides three modes for users to select including Port Forwarding, Port Mapping, and DMZ.

3.4.3.5.1 Port Forwarding



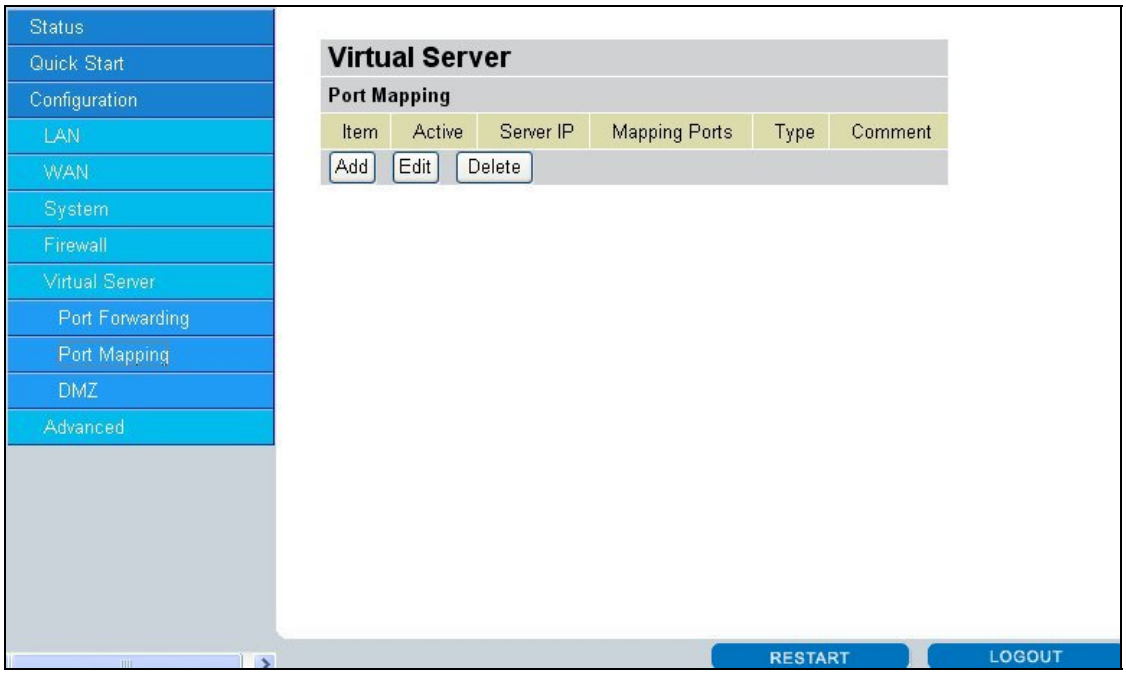


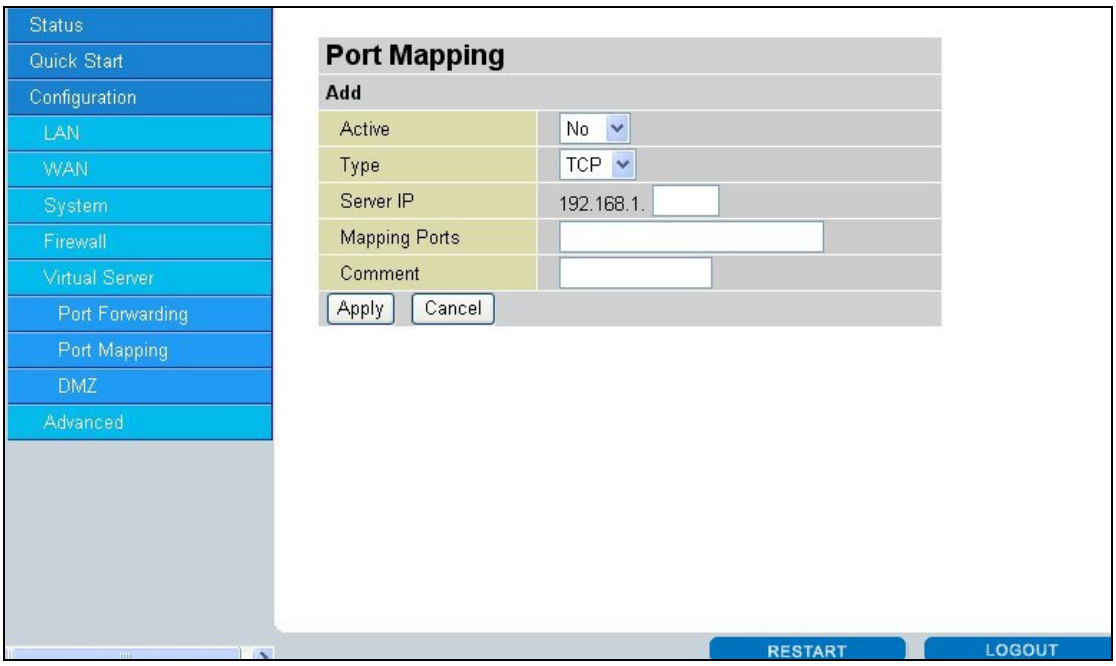
Type: Select **TCP** if you want to scope for the connection-based application service on remote server using the port number. Or select **UDP** if you want to scope for the connectionless application service on the remote server using the port number.

Private IP: Enter the IP address of certain internal server to which requests from the specified port is forwarded.

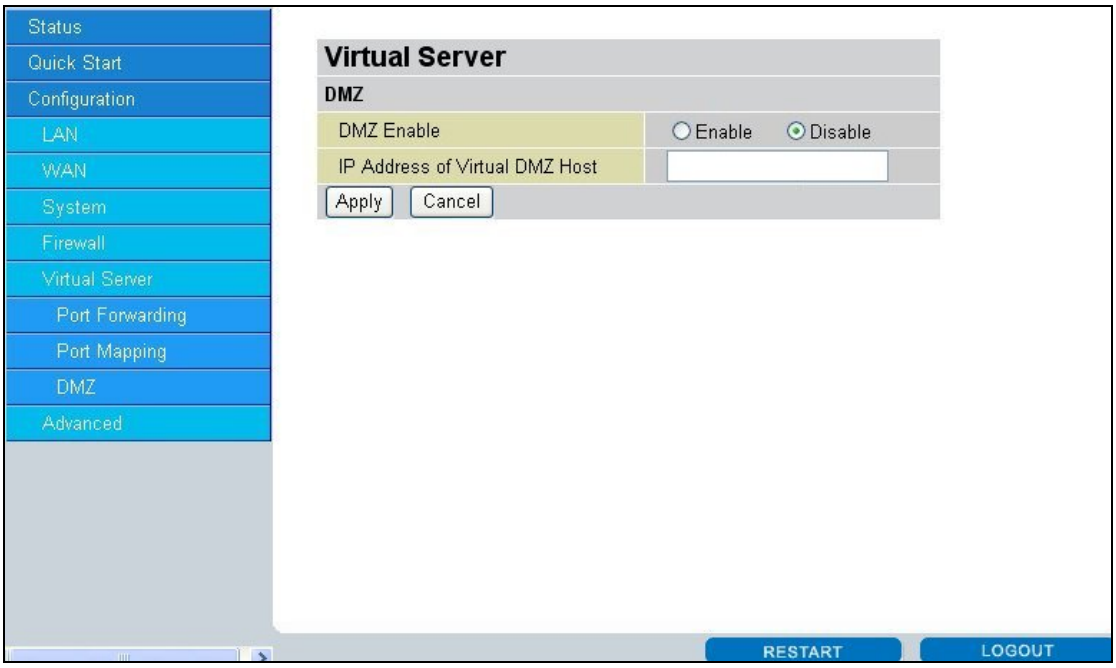
Public/Private Port: Enter the port number you want to configure.

3.4.3.5.2 Port Mapping





3.4.3.5.3 DMZ



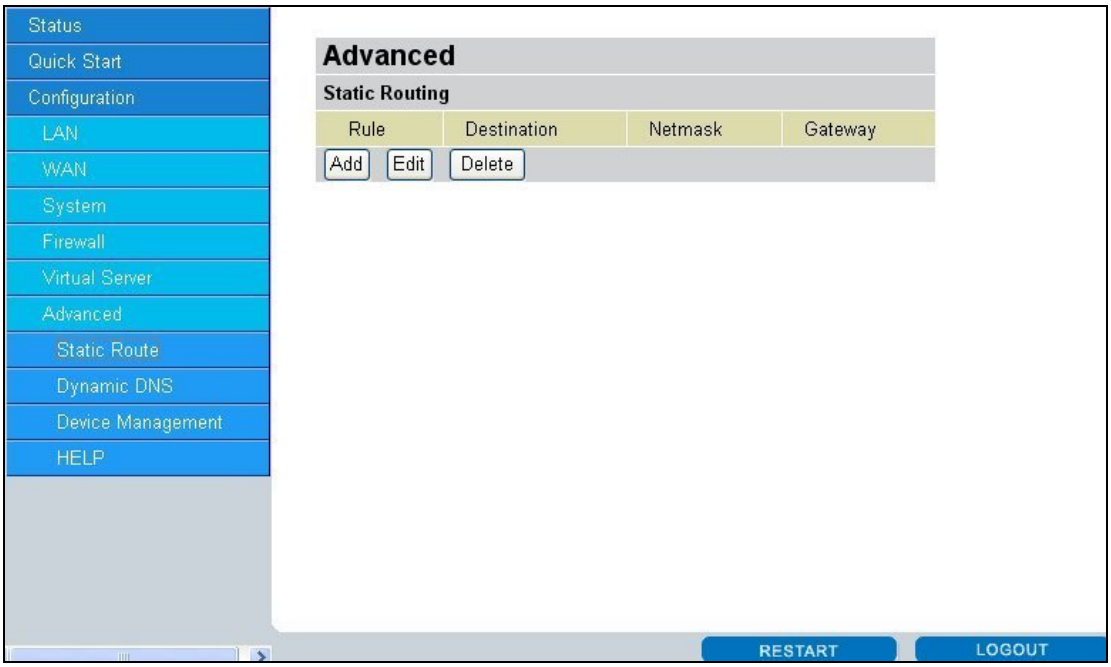
DMZ IP Address: Regarding the DMZ Host, it is a local computer exposed to the Internet. Therefore, an incoming packet will be checked by Firewall and NAT algorithms in the router, then passed to the DMZ host when packet is not sent from hacker and not matched by virtual server list.

3.4.3.6 Advanced

There are four items under the **Advanced** section: Static Route, Dynamic DNS, Device Management, and HELP.

3.4.3.6.1 Static Route

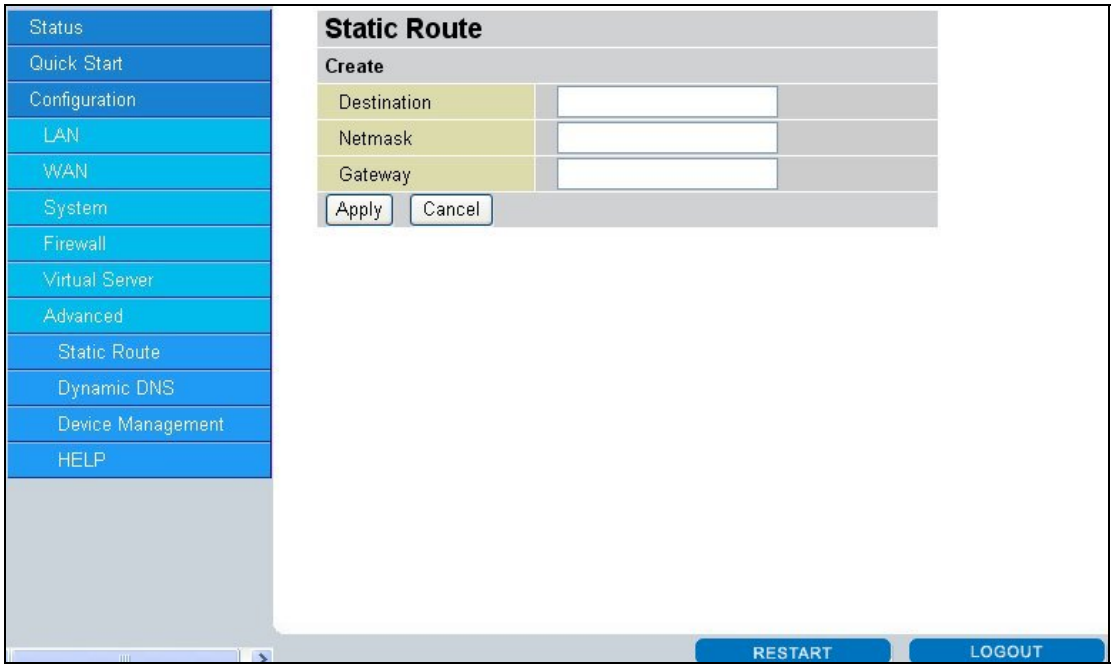
If you have another router with a LAN-to-LAN connection, you may create a static routing on the router that is the gateway to Internet.



Add: Click this button to add a new static routing. When you click this button, the next figure appears.

Edit: Check the item you want to edit. Then, click the “Edit” button.

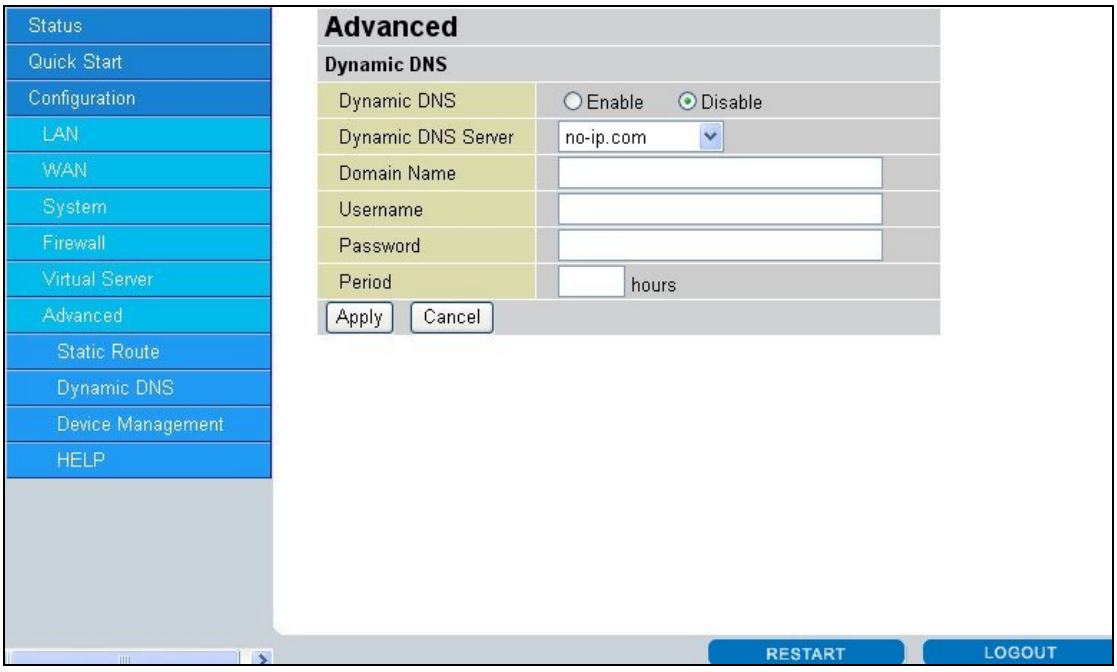
Delete: Check the item you want to delete. Then, click the “Delete” button.



Destination / Netmask / Gateway Address: Fill in these fields required by this Static Routing function.

3.4.3.6.2 Dynamic DNS

With Dynamic DNS service, a domain name can be translated into a dynamic IP address, which is often issued by ISP for dial-up service. A local server, such as Web server, Email server or FTP server, can then be easily accessed without knowing the changing IP address.



Dynamic DNS: Check the "**Enable**" button to access the Dynamic DNS service.

Dynamic DNS Server: You may sign up Dynamic DNS service at http://www.dyndns.org and there you can also register "domain names".

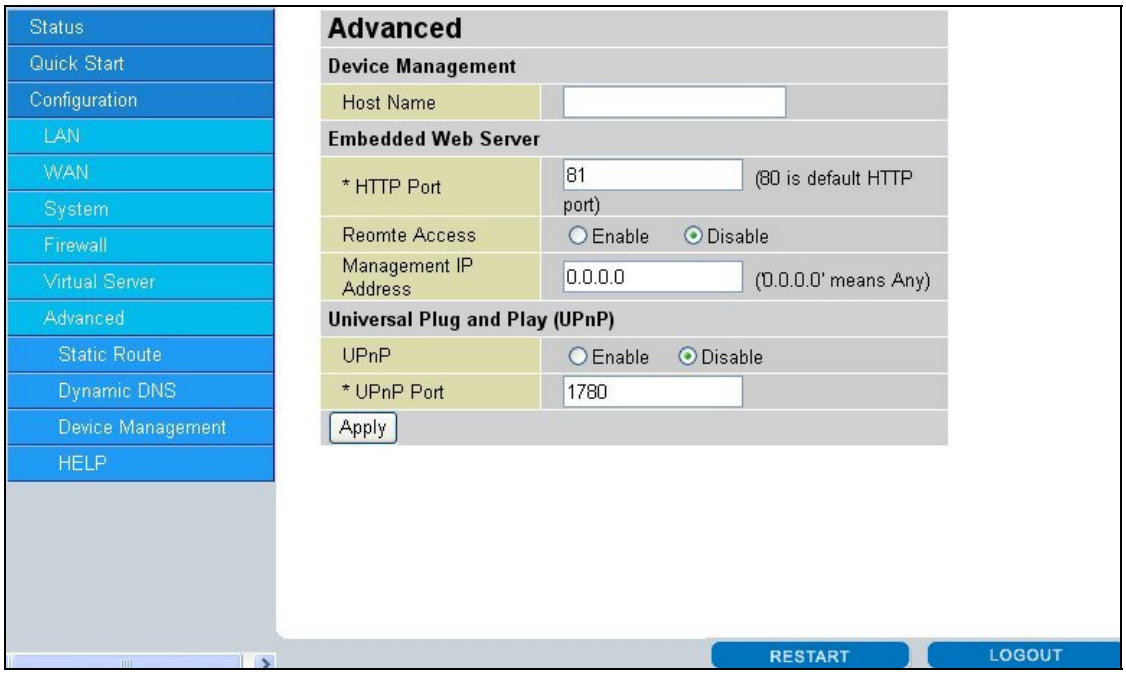
Domain Name: Enter one domain name you have registered.

User Name: Enter the username used for sign-up.

Password: Enter the password used for sign-up.

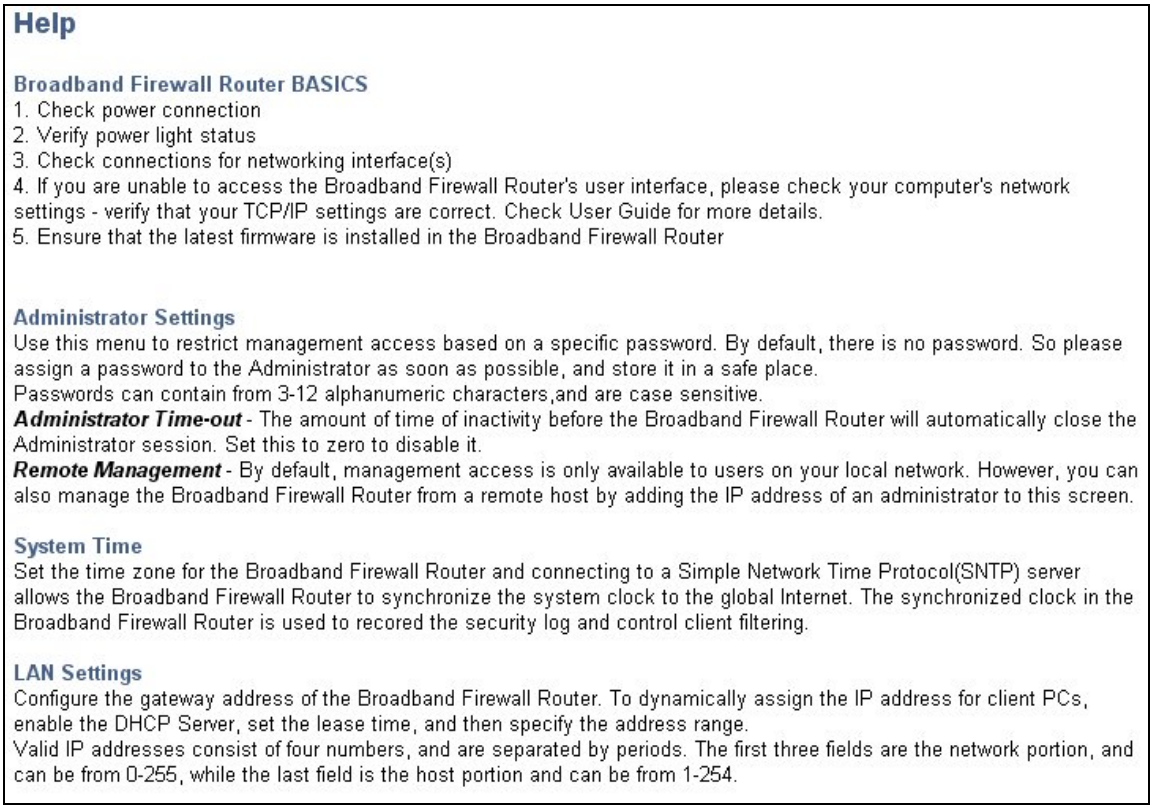
Period: Set the time period for the Router to exchange information with the DDNS server. In addition to update periodically according to this period setting, BIPAC 6600 will take the same action automatically whenever the assigned IP changes.

3.4.3.6.3 Device Management



3.4.3.6.4 HELP

After click on the hyperlink of "HELP" in the left pane, the following html page will jump out. This page would be a good reference for your preceding the configuration.



Help

Broadband Firewall Router BASICS

1. Check power connection
2. Verify power light status
3. Check connections for networking interface(s)
4. If you are unable to access the Broadband Firewall Router's user interface, please check your computer's network settings - verify that your TCP/IP settings are correct. Check User Guide for more details.
5. Ensure that the latest firmware is installed in the Broadband Firewall Router

Administrator Settings

Use this menu to restrict management access based on a specific password. By default, there is no password. So please assign a password to the Administrator as soon as possible, and store it in a safe place.
Passwords can contain from 3-12 alphanumeric characters,and are case sensitive.
Administrator Time-out - The amount of time of inactivity before the Broadband Firewall Router will automatically close the Administrator session. Set this to zero to disable it.
Remote Management - By default, management access is only available to users on your local network. However, you can also manage the Broadband Firewall Router from a remote host by adding the IP address of an administrator to this screen.

System Time

Set the time zone for the Broadband Firewall Router and connecting to a Simple Network Time Protocol(SNTP) server allows the Broadband Firewall Router to synchronize the system clock to the global Internet. The synchronized clock in the Broadband Firewall Router is used to recored the security log and control client filtering.

LAN Settings

Configure the gateway address of the Broadband Firewall Router. To dynamically assign the IP address for client PCs, enable the DHCP Server, set the lease time, and then specify the address range.
Valid IP addresses consist of four numbers, and are separated by periods. The first three fields are the network portion, and can be from 0-255, while the last field is the host portion and can be from 1-254.

Chapter 4
Troubleshooting

If the Broadband Router is not functioning properly, you can refer first to this chapter for simple troubleshooting before contacting your service provider. This could save your time and effort but if the symptoms persist, then consult your service provider.

Problems Starting Up the Broadband Router

Problem	Corrective Action
None of the LEDs are on when you turn on the Broadband Router.	Check the connection between the adapter and the Broadband Router. If the error persists, you may have a hardware problem. In this case, you should contact technical support.

Problems with the LAN Interface

Problem	Corrective Action
Can't ping any station on the LAN.	Check the LAN LNK LED on the front panel. The LED should be on for a port that has a station connected. If it is off, check the cables between your Broadband Router and the station.
	Verify that the IP address and the subnet mask are consistent between the Broadband Router and the workstations.

Why do I get IP conflict information in my computer?

When you see the message box prompted for IP address conflict in your computer, it could be caused by rebooting BIPAC 6600 or by two or more workstations occupying the same IP address. Please run the "**winipcfg**" utility to release all current configurations first, and then renew all if your computer is set to get an IP address automatically. BIPAC 6600 will assign a new IP address to your computer if DHCP server is enabled in the router. Furthermore, please double check each workstation's IP address from duplicate IP. The "winipcfg.exe" is used for Win95, 98, and ME. For WinNT,2000 and XP, please enter "ipconfig.exe".

Why won't my Internet application work?

To protect your computer from Hackers, the product uses port-blocking algorithm. A port likes a door into your computer. Each service on the Internet has an associated port. The product protects your computer by closing certain ports off so that malicious programs can't access your computer. Sometimes, however, you are using an application on purpose that uses one of these blocked ports. In this case you will have to manually open the port to allow the application to work properly.

Some applications that may be affected are
*Some **Email Programs***
*Some **Multi-Player Games***
*Some **Internet Phone/Video Conferencing Applications***

Also, there are some applications that require reverse connection over the Internet. In other words, when you are connected to these applications, you have to open your ports for forth and back connection.

The first thing you will need to do is determining what port or ports the application uses. Typically the fastest way to find this information is to go to the software maker's web site. Go to their support section and look for information related to NAT, Proxy Server, or Firewall. This information will typically list 1 to 3 ports that need to be opened for proper operation of the software. If you can't find the necessary information, call the software maker and ask what ports need to be opened for the software to work through a firewall.

Can I upgrade the gateway's firmware?

We provide two firmwares, one (*.bfw) is for boot code and the other (*.afw) is application code. Usually, you do not need to upgrade boot code in stead there is a specific description to upgrade boot code first for upgrading application code.

Can I set a fixed IP address on my PC?

Yes, you can configure your PC with fixed IP address. Specially, you need to setup a server explored to outside world. But be careful not to put fixed IP addresses into the DHCP IP pool. It may cause trouble. Again, this fixed IP address must be located within the same subnet as router IP setting.

For example, in the Windows 98, Go to Start -> Control Panel -> Network -> TCP/IP -> Properties -> ***IP address*** Tab, enter IP address as 192.168.1.1 (where router IP address is 192.168.1.254, subnet mask is 255.255.255.0, DHCP server's IP address pool from 192.168.1.100 to 192.168.1.199) and subnet mask as 255.255.255.0.

Next, in the ***DNS Configuration*** tab, enter your ISP DNS addresses or router's IP address (192.168.1.254). BIPAC 6600 has DNS relay function. It will relay your DNS request to real DNS server and send the result back to sender.

Finally, in the ***Gateway*** tab, enter the router's IP address (192.168.1.254) in this field and click Add button.

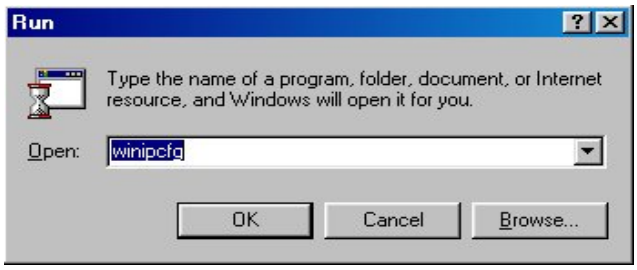
Is there a tool to check my PC's TCP/IP settings in MS Windows?

There are two programs we can use to display your current PC's TCP/IP settings.

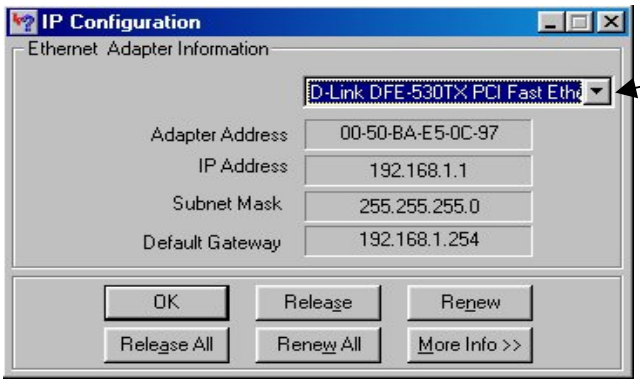
WINIPCFG.EXE

For Win95, 98, ME, the WINIPCFG program is used to gather information about the TCP/IP connections that are active on your system. It cannot be used to dynamically adjust TCP/IP connections. You can also renew leases (if allowed by the network), and get the current IP address assignments through this program.

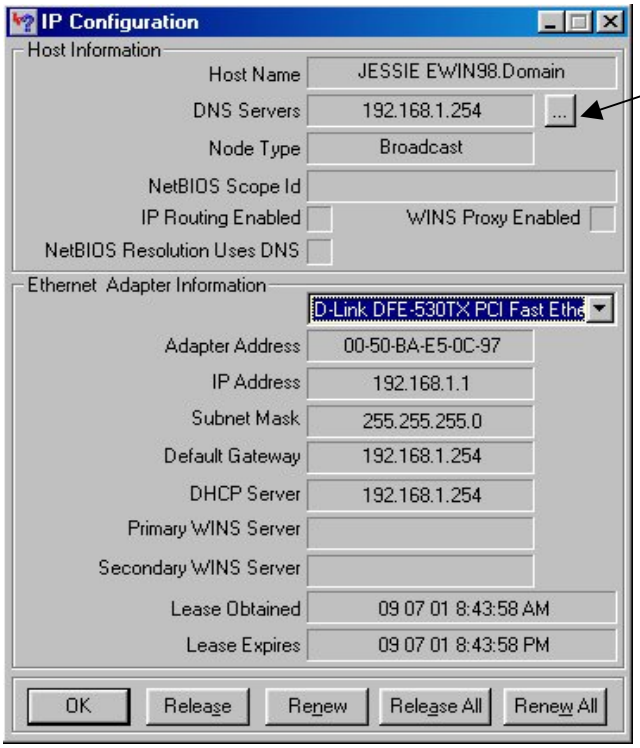
1. From Windows, go to **Start → Run**, enter **WINIPCFG,** and click **"OK"**.



2. The following figure displays the adapter address and current TCP/IP address. Select the correct Ethernet adapter that is installed in this computer at the "Ethernet Adapter Information".



3. Click the **"More Info >>"** button to get detailed configuration information.



4. On the top, the "Host Name" and "DNS server" of the computer are configured to call when it is looking for a named resource. The default gateway is the server through which the client connects to the Internet. The DHCP Server identifies the network server (i.e. BIPAC 6600) that assigns IP addresses to computers on the network.

If the product is working properly, the following should be apparent from this screen:

1) The Client should have an IP address within the prescribed range.

2) The "DHCP" and "Default Gateway" should list the product's local port address (the device's IP address).

3) The DNS server IP addresses should match the DNS server IP addresses set in the device.

IPCONFIG.EXE

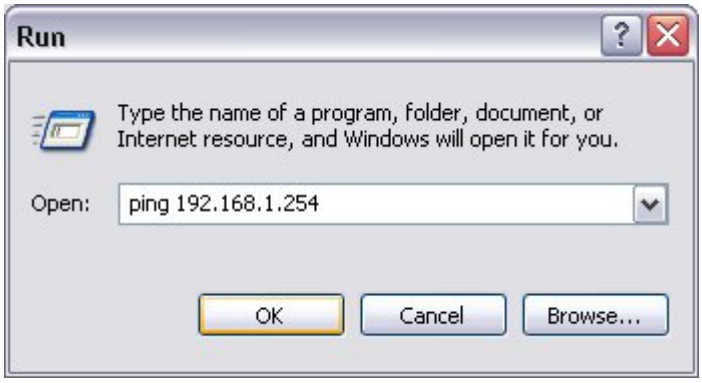
For WinNT, Win2000 and WinXP, go to **Start → Programs → Accessories → Command Prompt** to open the Command Prompt. Type in **IPCONFIG /ALL** and hit "Enter" to see the adapter's information. Type in **IPCONFIG /RELEASE** to release all adapters' IP address and **IPCONFIG /RENEW** to renew IP addresses. For a list of the **IPCONFIG** commands, type in **IPCONFIG /? .**

How can I test the whole path (PC←→Router←→outside world) to make sure it works fine?

There is a simple tool named PING. Send this command to desired IP station and should be immediately echoed back. Therefore it acts as a loop back. If you can receive the echo back successfully, the path is OK.

For example, you can enter PING command in MS-DOS prompt (or after choosing START_ RUN from the Start menu) as below in sequence.

- **PC to Router (e.g. ping 192.168.1.254)**



If there is no reply from router, please verify the PC, cables, HUB/Switch and router.

- **PC to external station with IP address (e.g. ping 168.95.192.1)**

If there is no reply from external station, please verify the router, cables, DSL/Cable modem, and connection protocols.

- **PC to external station with domain name (e.g. ping www.yahoo.comT)**

If there is no reply from external station, please verify the DNS setting in PC or router.

How can I check the active IP settings for my WAN port?

You may use the Web-based GUI to check the WAN port status, **Status -> System Log**, and then you will see whole process inside the router including the WAN port IP address and related information.

Where can I find the WAN port's MAC address?

When you need this WAN port MAC address, you can refer the MAC label in the enclosure. But the easiest way is to use Web-based GUI to check it. Please enter **Status -> Device Info** or **WAN -> Obtain an IP address automatically**, then you will see the MAC address for WAN port. Usually, some cable operators need this information for registration.

How can I explore a local server to be visible to outside users?

When being a natural Internet firewall (NAT + Advanced Firewall), BIPAC 6600 protects your network from being accessed by outside users. There is only one IP address visible to outside users who are not able to access the specific server in your LAN. When you need to allow outside users to access local servers, e.g. Web server, FTP server, E-mail server or News server. You can set up a local server with specific port number that stands for the service, e.g. Web (80), FTP (21), Telnet (23), SMTP (25), POP3 (110), DNS (53), ECHO (7), NNTP (119). Details are described in ***section 3.4.3.5 "Virtual Server"***. When an incoming access request to the router for specified port is received, it will be forwarded to the corresponding internal server.

For example, if you set the Service Port number 80 (Web) to be mapped to the IP Address 192.168.1.2, then all incoming requests with router's public IP address from outside users will be forwarded to the local server with IP address of 192.168.1.2.

What is DMZ host?

Regarding the DMZ Host (private IP address), it is a local computer exposed to the Internet. Therefore, an incoming packet will be checked by Firewall and NAT algorithms in the router, and then passed to the DMZ host when packet is not sent by hacker and not limited by virtual server list. Besides, there are some IP protocols that do not have port number information. There is no way to use Virtual Server setting to forward incoming packet. Therefore, DMZ host is the easy to forward this kind of packets. If you enable and set virtual server and DMZ host, the precedence is Virtual Server and then DMZ. For example, the incoming packet will be checked with Firewall rules, Virtual Server rules and then DMZ host.

How to configure my Mac OS to surf Internet through BIPAC 6600?

Please make sure the Mac OS open transport networking protocols is installed.

We will suggest that the router has DHCP server enabled and Mac OS gets an IP address automatically because Mac OS will get the other information at that same time, such as DNS IP address, subnet mask and Gateway IP address.

Click the Apple Manual -> Control Panel -> TCP/IP, and then

- Select **Connect via** : Ethernet
- Select **Configure** : Using DHCP server

If you select **Configure** as Manually, then you have to enter

- **IP Address** : 192.168.1.1
- **Subnet mask** : 255.255.255.0
- **Router address:** 192.168.1.254
- **Name server addr:** ISP's DNS IP addr or 192.168.1.254

Please refer above ***Question 7 "Can I set a fixed IP address on my PC?"*** for configuring manually.

How can I do if I forget the password for accessing Router?

If you ever forget the password to log in, you should contact the dealer where you bought this product.

How can I do if there is already a DHCP server in LAN?

If there are two DHCP servers existing in the same network, it may cause conflict and generate trouble. In this situation, we suggest to disable DHCP server in router and configure your PC manually as described in ***Question 7 "Can I set a fixed IP address on my PC?"***.

How many PCs can share this single BIPAC 6600 simultaneously?

Basically, it is depended on your subnet mask setting in router. For example, if you set 255.255.255.0 for subnet mask, router will allow up to 253 users to share the outgoing bandwidth. This is also the default setting in router.

Which connection method should I select in WAN-ISP setting window?

The broadband firewall router supports four kinds of access method to establish a connection as below.

PPPoE	Username, Password, Service Name, Domain Name System (DNS) IP address (it can be automatically assigned from ISP or be set fixed)
Fixed IP	IP address, Subnet mask, Gateway address, Domain Name System (DNS) IP address (it is fixed IP address)
Obtain an IP Address Automatically	Domain Name System (DNS) IP address (it can be automatically assigned from ISP or be set fixed)

APPENDIX

Product Support and Contact Information

Most problems can be solved by referring to the **Troubleshooting** section in the User's Manual. If you cannot resolve the problem with the **Troubleshooting** chapter, please contact the dealer where you purchased this product.

Contact Billion

WORLDWIDE

http://www.billion.com